Release Notes for Cisco ONS 15454 Release 7.0.2

September 2006

Release notes address closed (maintenance) issues, caveats, and new features for the Cisco ONS 15454 SONET multiplexer. For detailed information regarding features, capabilities, hardware, and software introduced with this release, refer to the "Release 7.0" version of the *Cisco ONS 15454 DWDM Installation and Operations Guide*; and the "Release 7.0" version of the *Cisco ONS 15454 Procedure Guide; Cisco ONS 15454 Reference Manual; Cisco ONS 15454 Troubleshooting Guide*; and *Cisco ONS 15454 SONET TL1 Command Guide*. For the most current version of the *Release Notes for Cisco ONS 15454 Release 7.0.2*, visit the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/ong/15400/454relnt/index.htm

Cisco also provides Bug Toolkit, a web resource for tracking defects. To access Bug Toolkit, visit the following URL:

http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

Contents

Changes to the Release Notes, page 2

Caveats, page 2

Resolved Caveats for Release 7.0.x, page 28

New Features and Functionality, page 32

Related Documentation, page 66

Obtaining Documentation, page 67

Documentation Feedback, page 68

Cisco Product Security Overview, page 68

Obtaining Technical Assistance, page 69

Obtaining Additional Publications and Information, page 71

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2006 Cisco Systems, Inc. All rights reserved.

Changes to the Release Notes

This section documents supplemental changes that have been added to the *Release Notes for Cisco ONS 15454 Release 7.0.2* since the production of the Cisco ONS 15454 System Software CD for Release 7.0.2.

The following changes have been added to the release notes for Release 7.0.2.

Changes to Caveats

The following caveats have been added.

CSCsd94528, page 2

CSCsf30853, page 4

CSCse47817, page 17

Caveats

Review the notes listed below before deploying the ONS 15454. Caveats with tracking numbers are known system limitations that are scheduled to be addressed in a subsequent release. Caveats without tracking numbers are provided to point out procedural or situational considerations when deploying the product.

Hardware

CSCsd94528

Intermittent Packet drops can occur when connecting a Catalyst Switch to a CE1000 during autonegotiation.

For more information review the following field notice:

FN - 62423 - 15454-CE-1000-4 Card Gets Burst Data from Incoming Source to FPGA of the CE-1000-4 Card Causing the Upper Layers of the Source to Resend

This issue is resolved in Release 8.0.

CSCed18803

Rarely, the non-enhanced Muxponder unit does not pass Jitter Tolerance test from Trunk port to client port as per ITU-T G.825, 2 Mb/s mask, at the 10 Hz specific setpoint. The Muxponder should be configured with G.709 Off, FEC Off and Trunk signal provided by external Jitter test box, and the unit client port output monitored for errors, to see this issue. This issue will not be resolved. Note that in normal network configurations the muxponder is operated with G.709 and FEC turned on, and the jitter tolerance tests pass.

CSCuk48503

Under specific conditions the non-enhanced MXPD does not pass the Telcordia GR-253/G.825 Jitter generation mask test on 10G TX Trunk port. The 2.5 G TX Client jitter generation is always within mask and does not exhibit this issue. This occurs only when, in SONET mode, there is no FEC, no G.709, and client interfaces are looped back, with non-synchronous clocking, and the jitter testbox TX connected to Trunk RX port, while the jitter testbox RX is connected to the Trunk TX port. The jitter testbox TX clock recovers from RX with an additional 5 ppm offset added. This issue will not be resolved.

CSCuk44284

An optical connector and optical attenuators inserted into the SFP may force the fiber against the shelf door when it is closed. Use the following types of optical connectors and optical attenuators when connecting to the SFP:

- **Optical connectors**: The length of the connector (starting from the ferule tip) plus the fiber boot must be 50 mm or shorter.
- **Optical Attenuators**: The following attenuator Cisco P/Ns are recommended:
  - 39-0228-XX
  - 39-0229-XX
  - 39-0230-XX

Jitter Performance with XC10G

During testing with the XC10G, jitter generation above 0.10 UI p-p related to temperature gradient testing has been observed. This effect is not expected to be seen under standard operating conditions. Changes are being investigated to improve jitter performance in a future release. Tracking numbers related to this issue include CSCdv50357, CSCdv63567, CSCdv68418, CSCdv68441, CSCdv68389, CSCdv59621, and CSCdv73402.

CSCdz49928

When using KLM type fuses with specific types of fuse and alarm panels, the PWR-REDUN alarm may not be displayed once the fuse is blown. A KLM fuse does not have a blown fuse indicator built into it. As a result, the blown fuse detection circuitry on the FAP may continue to provide voltage on its output despite a blown fuse.

Maintenance and Administration

Caution VxWorks is intended for qualified Cisco personnel only. Customer use of VxWorks is not recommended, nor is it supported by Cisco's Technical Assistance Center. Inappropriate use of VxWorks commands can have a negative and service affecting impact on your network. Please consult the troubleshooting guide for your release and platform for appropriate troubleshooting procedures. To exit without logging in, enter a Control-D (hold down the Control and D keys at the same time) at the Username prompt. To exit after logging in, type “logout” at the VxWorks shell prompt.

Note CTC does not support adding/creating more than 5 circuits in auto-ranged provisioning. This is as designed.

Note In releases prior to 4.6 you could independently set proxy server gateway settings; however, with Release 4.6.x and forward, this is no longer the case. To retain the integrity of existing network configurations, settings made in a pre-4.6 release are not changed on an upgrade to Release 7.0.x. Current settings are displayed in CTC (whether they were inherited from an upgrade, or they were set using the current GUI).

CSCsf30853

A DS3XM-12 card in portless mode does not send DS1 AIS on the DS1 ports when there is an incoming DS3 failure, such as DS3 AIS or DS3 MISM. The downstream DS1 facilities alarm is reported as LOF rather than AIS. This issue will be resolved in Releases 7.0.4 and 8.0.

CSCsc62845

When you try delete a provisionable patchcord (PPC) from the CTC Provisioning > PPC tab, sometimes CTC fails to refresh the screen and the PPC deletion appears to have failed. The workaround is to restart into CTC. This issue is resolved in Release 7.2.

CSCsc00811

Deleting a monitor circuit and its parent at the same time might result in a PARTIAL parent circuit. To avoid this, delete the monitor circuit before deleting the parent circuit. This issue will not be resolved

CSCsc36281

The software Activating progress popup window might fail to automatically close during multiple or parallel software activations. If this occurs you must manually close the popup window. The following error message might also be raised and need to be closed:

“EID-3251 Unable to complete requested action. Unable to activate because the working software version is newer than the protect one.”

To ensure that all nodes are using the correct software version you should close and restart CTC. This issue will be resolved in a future release.

Mismatch Equipment Attributes Alarm on EIA

In Release 6.0 a Mismatch Equipment Attributes (MEA) alarm is raised incorrectly against the B-Side BIC (EIA) on an ONS 15454 node using the 15454-SA-HD (high density) chassis with 1BNCB48, 1BNCB24, or 1SMBB84 EIAs installed. The 1BNCB48, 1BNCB24, and 1SMBB84 EIA panels are compatible with the 15454-SA-HD shelf assembly; however, the software in Release 6.0 fails to recognize their compatibility. The MEA alarm raised as a result of this issue is not service impacting, but does cause a standing alarm.

As a workaround to the standing alarm, you can change the BIC-MEA alarm severity by creating and using a custom alarm profile following the steps that apply for your network in the NTP-A71 Create, Download, and Assign Alarm Severity Profiles procedure of the Manage Alarms chapter in the Cisco ONS 15454 Procedure Guide, Release 6.0. This issue will be resolved in Release 6.1.

CSCeh84908

A CTC client session can disconnect from an ONS node during simultaneous deletion of large numbers of VT level circuits (3000+). Connectivity to the node will recover without any user action. If the condition persists, restart the CTC session to reconnect. This issue is under investigation.

CSCei36415

When retrieving GBIC inventory for the FC_MR-4, nothing is returned for the CLEI code. In a future release, enhanced inventory information will be available for ONS GBICs. This will include the CLEI code.

CSCeh92201

When you create a bidirectional BLSR-UPSR IDRI circuit using autorouting and select the PCA option for secondary spans, the circuit is created over working BLSR spans and does not use PCA spans. To enforce the use of the PCA option, provision the circuit using manual routing. This issue will not be resolved.

CSCee96164

The Wait To Restore (WTR) alarm does not appear to be raised for as long as the WTR timer is set for. The WTR is raised correctly, but the alarm is hidden for the first 12 seconds due to the clear soaking time for a CLDRESTART alarm. You can see this behavior if you set up a 1+1 bidirectional revertive protection group, remove the working card, and then reinsert the card. There are no plans to change this behavior.

CSCee25136

If you create a PM schedule with the Start time for the PM report equal to 00:00 (in TL1, “0-0”), after a few minutes the PM report start time might change to 23:59 (in TL1, “23-59”). This issue will not be resolved.

CSCed23484

A user might remain in the logged-in state after rebooting the PC while logged into a node running CTC. The user login will time out once the “Idle User Timeout” limit is up. Alternatively, you can log in as a superuser and force the user off. This issue will not be resolved.

CSCds88976

When a new circuit is created around a ring (UPSR or BLSR), the SD BER or SF BER alarm can be raised depending on the order in which the spans are provisioned. The alarms will eventually clear by themselves. Traffic is not affected. This issue will not be resolved.

CSCdu82934

When you auto-route a VT circuit on an ONS 15454 node, a path is computed based on the availability of STSs on the nodes involved. This selection process, when combined with a lack of VT matrix (or STS-VT connections) on an auto-route selected node, can result in the VT circuit creation failing with the message “unable to create connection object at node.” To correct this situation, manually route VT circuits in cases when auto-routing fails. The error message will indicate which node is at issue.

CSCef28522

When you inject errors on a splitter protection card in the node's working port, CVL and ESL are incremented for the working and protect far end ports. This issue will not be resolved.

CSCuk49106

The amplifier gain set point shown by CTC and the actual measured amplifier gain differ. The following steps illustrate this issue.

Step 1 Reduce the insertion loss of the span just before the amplifier.

Step 2 Execute the APC procedure.

The APC procedure does not check consistency between the gain set point and the real gain, but rather only verifies the amplifier total output power. As a workaround, manual setting can be performed to align these values, although the discrepancy does not impact the normal functioning of the amplifier. This issue will not be resolved.

CSCef05162

Clearing the displayed statistics for a port will also clear the displayed history for that port. Clearing the displayed statistics for all ports will also clear the displayed history for all ports. There is no warning message from the TCC2. If History information is to be retained, do not clear displayed statistics for any port without first documenting the displayed history information for the associated port. This issue will not be resolved.

CSCef29516

The ALS pulse recovery minimum value is 60 instead of 100. If this occurs, increase the value to 100. This issue will not be resolved.

CSCeb36749

In a Y-Cable configuration, if you remove the client standby RX fiber; a non-service affecting LOS is raised, as expected. However, if you then remove the trunk active RX fiber; a non-service affecting LOS-P is raised, but the previously non-service affecting LOS on the client port is now escalated to a service affecting alarm, in spite of no traffic having been affected. This issue will not be resolved.

CSCee82052

After setting the node time (either manually or via NTP) you must wait for the endpoint of the interval to be reached before the end time will reflect the recently-set node time. Until this has occurred, the date time stamp for the end of the retrieved interval remains 12/31/69. This issue has been closed and will not be resolved.

CSCdx35561

CTC is unable to communicate with an ONS 15454 that is connected via an Ethernet craft port. CTC does, however, communicate over an SDCC link with an ONS 15454 that is Ethernet connected, yielding a slow connection. This situation occurs when multiple ONS 15454s are on a single Ethernet segment and the nodes have different values for any of the following features:

- Enable OSPF on the LAN
- Enable Firewall
- Craft Access Only

When any of these features are enabled, the proxy ARP service on the node is also disabled. The ONS 15454 proxy ARP service assumes that all nodes are participating in the service.

This situation can also occur immediately after the aforementioned features are enabled. Other hosts on the Ethernet segment (for example, the subnet router) may retain incorrect ARP settings for the ONS 15454s.

To avoid this issue, all nodes on the same Ethernet segment must have the same values for Enable OSPF on the LAN, Enable Firewall, and Craft Access Only. If any of these values have changed recently, it may be necessary to allow connected hosts (such as the subnet router) to expire their ARP entries.

You can avoid waiting for the ARP entries to expire on their own by removing the SDCC links from the affected ONS 15454 nodes. This will disconnect them for the purposes of the proxy ARP service and the nodes should become directly accessible over the Ethernet. Network settings on the nodes can then be provisioned as desired, after which the SDCC can be restored.

This issue will not be resolved.

CSCdy56693

Microsoft Windows XP uses more memory than previous Microsoft operating systems, and this may result in reduced CTC performance. To avoid reduced performance, you can:

- Limit the number of nodes you log into
- Avoid or limit bulk operations
- Avoid bulk circuit deletion
- Prevent CTC's discovery of DCC connected nodes by using the login "Disable Network Discovery" feature
- Prevent CTC's discovery of circuits unless needed by using the login "Disable Circuit Management"

CSCdy62092

When a node connected via SDCC has no Ethernet LAN connectivity, display of SDCC termination alarms is delayed if the fiber connecting a DCC connected node is removed. This issue cannot be resolved.

CSCdy10030

CVs are not positively adjusted after exiting a UAS state. When a transition has been made from counting UAS, at least 10 seconds of non-SES must be counted to exit UAS. When this event occurs, Telcordia GR-253 specifies that CVs that occurred during this time be counted, but they are not. There are no plans to resolve this issue at this time.

CSCdy11012

When the topology host is connected to multiple OSPF areas, but CTC is launched on a node that is connected to fewer areas, the topology host appears in CTC, and all nodes appear in the network view, but some nodes remain disconnected. This can occur when the CTC host does not have routing information to connect to the disconnected nodes. (This can happen, for example, if automatic host detection was used to connect the CTC workstation to the initial node.)

CTC will be able to contact the topology host to learn about all the nodes in all the OSPF areas, but will be unable to contact any nodes that are not in the OSPF areas used by the launch node. Therefore, some nodes will remain disconnected in the CTC network view.

To work around this issue, if no firewall enabled, then the network configuration of the CTC host can be changed to allow CTC to see all nodes in the network. The launch node must be on its own subnet to prevent network partitioning, and craft access must not be enabled. The CTC host must be provisioned with an address on the same subnet as the initial node (but this address must not conflict with any other node in the network), and with the default gateway of the initial node. CTC will now be able to contact all nodes in the network.

If a firewall is enabled on any node in the network, then CTC will be unable to contact nodes outside of the initial OSPF areas. This issue will not be resolved.

NE Defaults

The following caveats apply for NE defaults when managing older, pre-Release 4.5 nodes.

- OC12-4 allows provisioning of PJStsMon from 0 to 48. The workaround is to limit provisioning to between Off and 1 to 12 only.
- CTC displays “PJStsMon=off” in the standard provisioning pane when provisioning PJStsMon off; however, TL1 and the NE Defaults editor both display 0 for this same condition.
- If you only make changes to a single default in the NE defaults editor, you must click on another default or column before the Apply button becomes functional.

ONS 15454 Conducted Emissions Kit

If you are deploying the Cisco ONS 15454 within a European Union country that requires compliance with the EN300-386-TC requirements for Conducted Emissions, you must obtain and install the Cisco ONS 15454 Conducted Emissions kit (15454-EMEA-KIT) in order to comply with this standard.

CSCdv10824: Netscape Plugins Directory

If you use CTC, JRE, and the Netscape browser with a Microsoft Windows platform, you must ensure that any new installation of Netscape uses the same Netscape directory as the previous installation did, if such an installation existed. If you install Netscape using a different path for the plugins directory, you will need to reinstall JRE so that it can detect the new directory.

"Are you sure" Prompts

Whenever a proposed change occurs, the "Are you sure" dialog box appears to warn the user that the action can change existing provisioning states or can cause traffic disruptions.

Common Control Cards

CSCdw27380

Performing cross connect card switches repeatedly might cause a signal degrade condition on the lines or paths that can trigger switching on these lines or paths. If you must perform repeated cross connect card switches, lock out the corresponding span (UPSR, BLSR, or 1+1) first. This issue will not be resolved.

Active Cross Connect (XC10G/XCVT) or TCC2/TCC2P Card Removal

You must perform a lockout in BLSR, UPSR, and 1+1 before physically removing an active cross connect (XC10G/XCVT) or TCC2/TCC2P card. The following rules apply.

Active cross connect (XC10G/XCVT) cards should not generally be physically removed. If the active cross connect or TCC2/TCC2P card must be removed, you can first perform an XCVT/XC10G side switch or TCC2/TCC2P reset and then remove the card once it is in standby, or you can perform a lockout on all circuits that originate from the node whose active cross connect or active TCC2/TCC2P will be removed (performing a lockout on all spans will also accomplish the same goal). No lockout is necessary for switches initiated through CTC or through TL1.

Caution If you mistakenly remove an active TCC2/TCC2P card and you subsequently lose traffic on some interface cards, you may need to physically reset these cards if they fail to regain traffic.

Ethernet Polarity Detection

The TCC2/TCC2P does not support Ethernet polarity detection. The TCC+ and TCCI both support this feature. If your Ethernet connection has the incorrect polarity (this can only occur with cables that have the receive wire pairs flipped), the TCC+/I will work, but the TCC2/TCC2P will not. In this event, a standing condition, "LAN Connection Polarity Reverse Detected" (COND-LAN-POL-REV), will be raised (a notification will appear on the LCD, and there will be an alarm raised). This issue will most likely be seen during an upgrade or initial node deployment. To correct the situation, ensure that your Ethernet cable has the correct mapping of the wire wrap pins. For Ethernet pin mappings, consult the user documentation.

Optical IO Cards

CSCei26718

On the 15454_MRC-12, when a one way VT/VC circuit on UPSR over 1+1 protection is

created, the alarm behavior is not the same as in two way circuit creation. In particular, for the one way circuit creation, UNEQ-V and PLM-V alarms are reported, and the circuit state remains OOS. This issue will not be resolved.

CSCdw66444

When an SDH signal is sent into an ONS 15454 OC-12/STM-4 (IR, 1310 LR and 1550 LR) or an OC-48/STM-16 high-speed (IR and LR) port which has been configured to support SDH, an SD-P (Signal Degrade) alarm will appear as soon as the circuit is created. This alarm will continue to exist until the circuit is deleted.

To avoid this problem, when provisioning an OC-12/STM-4 (IR, 1310 LR and 1550 LR) or an OC-48/STM-16 high-speed (IR and LR) port to support SDH, disable the signal degrade alarm at the path level (SD-P) on the port.

Also, PM data at the path level will not be reliable. You must set associated threshold values to 0 in order to avoid threshold crossing alerts (TCA) on that port. The path threshold values to set to zero are CV-P, ES-P, SES-P, and UAS-P.

These issues are the result of a hardware limitation, and there are no current plans to resolve them.

CSCdw09604

If you are using an XC10G with OC-48, you must use either OC-48AS or OC-48 cards with a revision number higher than 005D.

Electrical IO Cards

CSCsc65320 and CSCin92295

In a DS3-EC1-48 1:N protection group for which a UPSR circuit drops onto a 1:N protected card, if you remove the card and then reseat it the switch time might exceed 60 ms. This issue will be resolved in a future release.

CSCsc60437

DS3XM one way circuits created with no electrical lines attached to the ports fail to carry traffic. This issue will be resolved in Release 8.0.

CSCei59527

When an XC switch occurs, LOF is driven to the line side. On a DS1-14 this can cause us to see long switch times that are related to hardware issues if the “Treat LOF as a Defect” flag has been set. To avoid this issue, do not set the “Treat LOF as a Defect” flag to true on DS1-14 cards. A future release will remove the “Treat LOF as a Defect” option for this card.

CSCeh43011

An LOS alarm is cleared when switching to protect when the working card is on opposite side of the shelf from the protect card (in portless configuration) in a DS3XM-12 1:N protection group. An electrical port brought into IS state on the portless only card produces an LOS alarm. If you then switch to protect, the alarm appears to clear. To avoid this issue, do not bring electrical ports into IS state on a portless only card. This issue will be resolved in a future release.

CSCdx40300

A transient WKSWPR condition is raised upon deletion of a DS3XM 1:1 protection group. This issue will be resolved in a future release.

CSCec39567

Deleting a DS3I 1:N protection group may leave the protect card LED in a standby state. This can occur in a DS3I 1:N protection group with a LOCKON applied to the working card (ONS 15454 ANSI chassis only). Upon deleting the protection group, the LED on the protect DS3I card and the CTC display are still in the standby state. Soft reset the protect card to update the LED on the card and in CTC. An alternative workaround is to remove the LOCKON before deleting the protection group. This issue will be resolved in a future release.

Data IO Cards

SONET and SDH Card Compatibility

Tables 1, 2, and 3 list the cards that are compatible for the ONS 15454 SONET and ONS 15454 SDH platforms. All other cards are platform specific.

Table 1 SDH Data Cards that are SONET Compatible

Product Name	Description
15454E-G1000-4	4 port Gigabit Ethernet Module - need GBICs
15454E-E100T-12	12 port 10/100BT Ethernet Module
15454E-E1000-2	2 port Gigabit Ethernet Module - need GBICs
15454E-ML100T-12	10/100 Mbps Ethernet card, 12 ports, RJ-45, L2/L3 switching, SDH/ETSI system, includes console cable
15454E-ML1000-2	1000 Mbps Ethernet card, 2 SFP slots, L2/L3 switching, SDH/ETSI system

Table 2 SONET Data Cards that are SDH Compatible

Product Name	Description
CE-1000-4	4 port 1000-Mbps Gigabit Ethernet module
CE-100T-8	8 port 10/100FE Ethernet module
15454-G1000-4	4 Port Gigabit Ethernet
15454-E100T-G	10/100BT, 12 circuit, compatible w/ XC, XCVT and XC10G
15454-E1000-2-G	Gigabit Ethernet, 2 circuit, GBIC - G
15454-ML100T-12	10/100 Mbps Ethernet card, 12 ports, RJ-45, L2/L3 switching, SONET/ANSI system, includes console cable
15454-ML1000-2	1000 Mbps Ethernet card, 2 SFP slots, L2/L3 switching, SONET/ANSI system

Table 3 Miscellaneous Compatible Products

Product Name	Description
15454-BLANK	Empty slot Filler Panel
15454-GBIC-LX	1000Base-LX, SM or MM, standardized for 15454/327
15454-GBIC-SX	1000Base-SX, MM, standardized for 15454/327
15454-FIBER-BOOT=	Bag of 15 90 degree fiber retention boots
15454-SFP-LC-SX	1000BASE, SX, short-reach, multimode, small form factor pluggable (SFP), LC connectors
15454-SFP-LC-LX	1000BASE, LX, long-reach, single mode, SFP, LC connectors
15454-CONSOLE-02	Cable, console, ML-Series, RJ-11 plug to RJ-45 jack, 22in/55.9cm long, SONET/ANSI system
15454E-CONSOLE-02	Cable, console, ML-Series, RJ-11 plug to RJ-45 jack, 22in/55.9cm long, SDH/ETSI system

CSCsc11981

Under certain circumstances, E-series cards might learn invalid MAC addresses and temporarily lose well-known/static addresses, possibly resulting in high flood rates. This issue can occur when traffic flows through an E-series card and there are no MAC addresses currently in the MAC table for that E-series card (for instance, after you have cleared the complete MAC table, or when the node is just coming up). The chipset can cause the E-series card to learn invalid addresses in this scenario under high rates of flood traffic (multicast, broadcast, unknown) or PHY interface noise. Side-effects of clearing the MAC table when traffic is flowing can cause the E-series card to lose well-known/static MAC addresses along with dynamically learned MAC addresses. This can cause high flood rates (multicast, broadcast, unknown) possibly reaching the limitation described in the following field notice:

http://www-tac.cisco.com/Support_Library/field_alerts/fn13171.html

This issue can last for a few seconds (typically less). The workaround is to avoid issuing any operation (such as the “Clear all MAC” command) that clears the complete MAC table under heavy traffic loads. To recover from this issue, wait for a few seconds to let the invalid addresses age out, and to allow the software to restore the well-known/static MAC addresses.

CSCdy37198

On Cisco ONS 15454s equipped with XCVT cross-connect cards, neither the E100T-12 nor the E1000-2 cards raise an alarm or condition in CTC when Ethernet traffic is predictably lost due to the following circumstances:

Circuits exist between Ethernet cards (E100T-12 and/or E1000-2) built over Protection Channel Access (PCA) bandwidth on BLSR spans. When BLSR issues a switch, the PCA bandwidth is preempted. Since there is no longer a connection between the ends of the Ethernet circuit, traffic is lost.

Note In nodes equipped with XC10G, these Ethernet cards will raise an AIS-P condition.

This issue will not be resolved.

CSCdr94172

Multicast traffic can cause minimal packet loss on the E1000-2, E100-12, and E100-4 cards. Packet loss due to normal multicast control traffic should be less than 1%. This issue was resolved in Release 2.2.1 for broadcast, and in Release 2.2.2 for OSPF, and some multicast frames. As of Release 3.0.3, the ONS 15454 supports HSRP, CDP, IGMP, PVST, and EIGRP, along with the previously supported broadcast and OSPF.

Note If multicast is used for such applications as video distribution, significant loss of unicast and multicast traffic will result. These cards were not designed for, and therefore should not be used for, such applications.

Note If the multicast and flood traffic is very rare and low-rate, as occurs in most networks due to certain control protocols and occasional learning of new MAC addresses, the loss of unicast frames will be rare and likely unnoticeable.

Note A workaround for this issue is to use the port-mapped mode of the E-series cards.

Multicast MAC addresses used by the control protocols in Table 4 have been added to the static MAC address table to guarantee no loss of unicast traffic during normal usage of these MAC addresses.

Table 4 Protocols Added to the MAC Address Table

Protocol	Release Protocol Introduced In
Broadcast MAC (used by many protocols)	2.2.1
Open Shortest Path First (OSPF)	2.2.2
Cisco Discovery Protocol (CDP)	2.2.2
Per-VLAN Spanning Tree (PVST)	2.2.2
Enhanced Interior Gateway Routing Protocol (EIGRP)	2.2.2
Internet Group Management Protocol (IGMP)	2.2.2
Hot Standby Routing Protocol (HSRP)	3.0.3

E1000-2/E100T

Do not use the repair circuit option with provisioned stitched Ethernet circuits.This issue is under investigation.

Single-card EtherSwitch

Starting with Release 2.2.0, each E100/E1000 card can be configured as a single-card EtherSwitch configuration to allow STS-12c of bandwidth to be dropped at each card. The following scenarios for provisioning are available:

1. 12c
2. 6c, 6c
3. 6c, 3c, 3c
4. 6c, six STS-1s
5. 3c, 3c, 3c, 3c
6. 3c, 3c, six STS-1s
7. Twelve STS-1s

When configuring scenario 3, the STS-6c must be provisioned before either of the STS-3c circuits.

Multicard EtherSwitch

When deleting and recreating Ethernet circuits that have different sizes, you must delete all STS circuits provisioned to the EtherSwitch before you create the new circuit scenario. (See the preceding "Single-card EtherSwitch" section for details on the proper order of circuit creation.) Enable front ports so that the VLANs for the ports are carried by the largest circuit first. A safe approach is to enable the front port before you create any circuits and then retain the front port VLAN assignment afterwards. If you break the rules when creating a circuit, or if you have to delete circuits and recreate them again, delete all circuits and start over with the largest first.

CSCds02031 and CSCsb49501 E1000-2/E100

When you drop two 3c multicard EtherSwitch circuits onto an Ethernet card and delete only the first circuit, you should not provision STS-1 circuits to the card without first deleting the remaining STS-3c circuit. If you attempt to create an STS-1 circuit after deleting the first STS-3c circuit, the STS-1 circuit will not work and no alarms will indicate this condition. Under rare conditions, this could trigger a TCC reset. To avoid a failed STS-1 circuit and other possible problems, delete the second STS-3c prior to creating any STS-1 circuit.

CSCed96068

If an ML-Series card running Software Release 4.6.2 or later is interoperating with an ML-Series card running Software Release 4.6.0 or 4.6.1, then the pos vcat resequence disable command must be added to the configuration of the ML-Series card running R4.6.2 or later. For documentation of this command, consult the *Ethernet Card Software Feature and Configuration Guide*.

CSCec52443

On an ML-series RPR ring circuit deletion or creation causes an approximately 200 ms traffic loss. To avoid this issue, from the ML-series CLI, perform a “shutdown” on both ends of the circuit prior to circuit changes. This issue will not be resolved.

CSCec52372

You must issue a “shut” command to both ends of a POS circuit before placing the circuit OOS, and issue IS before a “no shut” command. Placing a POS circuit OOS without shutting down can cause long traffic hits. This issue will not be resolved.

CSCec51252

You must issue a “shut” on both ends of affected POS circuits before performing a maintenance action on those circuits. If a POS circuit is restored without first issuing the shut commands, one end of the circuits could come up before the other. During that time, traffic is lost because the other end is not up yet. This issue will not be resolved.

CSCea46580

SPR input counters do not increment on a BVI with an SPR interface. This issue will not be resolved.

CSCea35971

A monitor command may disappear from the configuration after a TCC reboots. To avoid this issue, use the exec command, “terminal monitor,” instead (a minor drawback is that this command applies to all VTYs), or, alternatively, reapply the monitor command after connection is lost. This is as designed.

CSCdz49700

The ML-series cards always forward Dynamic Trunking Protocol (DTP) packets between connected devices. If DTP is enabled on connected devices (which might be the default), DTP might negotiate parameters, such as ISL, that are not supported by the ML-series cards. All packets on a link negotiated to use ISL are always counted as multicast packets by the ML-series card, and STP and CDP packets are bridged between connected devices using ISL without being processed. To avoid this issue, disable DTP and ISL on connected devices. This functionality is as designed.

CSCdz68649

Under certain conditions, the flow-control status may indicate that flow control is functioning, when it is not. Flow-control on the ML-series cards only functions when a port-level policer is configured. A port-level policer is a policer on the default and only class of an input policy-map. Flow-control also only functions to limit the source rate to the configured policer discard rate, it does not prevent packet discards due to output queue congestion.

Therefore, if a port-level policer is not configured, or if output queue congestion is occurring, policing does not function. However, it might still mistakenly display as enabled under these conditions. To avoid this issue, configure a port-level policer and prevent output queue congestion. This issue will not be resolved.

CSCdz69700

Issuing a **shutdown**/**no shutdown** command sequence on an ML1000 port clears the counters. This is a normal part of the startup process and there are no plans to change this functionality.

CSCin29274

When configuring the same static route over two or more interfaces, use the following command:

ip route *a-prefix a-networkmask a.b.c.d*

Where *a.b.c.d* is the address of the outgoing gateway, or, similarly, use the command:

ip route vrf *vrf-name*

Do not try to configure this type of static route using only the interface instead of the address of the outgoing gateway. This issue will not be resolved.

CSCin32057

If no BGP session comes up when VRF is configured and all interfaces have VRF enabled ensure that at least one IP interface (without VRF) is configured and add an IP loopback interface on each node. This issue will not be resolved.

CSCdy47284

ML-100 FastEthernet MTU is not enforced. However, frames larger than 9050 bytes may be discarded and cause Rx and Tx errors. This issue will not be resolved.

CSCdz74432

Issuing a “clear IP route *” command can result in high CPU utilization, causing other processes to be delayed in their execution. To avoid this issue do not clear a large number of route table entries at once, or, if you must use the “clear IP route *” command, do not install more than 5000 EIGRP network routes.

DWDM Cards

CSCse47817

When you attempt to change the MinExpSpan or MaxExpSpan values the wrong error message might be displayed as follows:

“EID-6151” the Min Span loss must be less than the max loss

This message appears even if the measured value is in the correct range. This issue is resolved in Releases 7.0.2 and 8.0.

CSCse41468

The GE interface remains down on a switch connected to an MXP_MR_2.5G card. This can occur during failure recovery with AUTO NEGOTIATION enabled on a connected switch. To work around this issue disable AUTO NEGOTIATION or set sync-restart-delay 10000 on the port of the switch. This issue will not be resolved.

CSCeh22604

When an MXP_MR_2.5G card is in MIXED or ESCON mode, TCA and alarm optical thresholds of Tx power for laser bias are configurable for ESCON payload, though not supported. This issue will be resolved in the future release.

CSCei19148

When a port is placed in-service while the conditions necessary to squelch the port are present, as in when the trunk port on a DWDM card is OOS,DSBLD and a client port is placed in-service, the client will momentarily enable, emitting light, before squelching due to the trunk OOS,DSBLD condition. The pulse is approximately 500 ms. This issue will not be resolved.

CSCei87554

When using a 1GE payload over the TXP_MR_2.5G the IfInErrors counter does not report oversized, undersized, or CRC errored frames, but rather, reports frame coding only. This issue will not be resolved.

CSCsb47323

For MXP_MR_10DME-C and MXP_MR_10DME-L cards, an unexpected RFI condition might be raised along with an OTUk-BDI. When there is an LOS downstream, the node receives OTUk-BDI. Because of the placement of dual OTN and SONET wrappers, it can also receive an RFI. This issue will not be resolved.

CSCsb79548

A long traffic hit can occur when an active TCC2/TCC2P resets while an MXP_MR_10DME-C or MXP_MR_10DME-L card is rebooting.

This issue can be reproduced as follows:

Step 1 1. Set up two MXP_MR_10DME-C or MXP_MR_10DME-L cards, connected back-to-back in two different nodes, A and B.

Step 2 2. Ensure that Node A has two TCC2 cards; one is active, and the other is standby.

Step 3 3. Set up any kind of traffic between the two MXP_MR_10DME-C or MXP_MR_10DME-L cards.

Step 4 4. Soft reset the MXP_MR_10DME card in Node A, then soft reset the active TCC2/TCC2P.

OTUk/ODUk-SD, FEC Uncorrected word alarms are raised on the trunk port. Traffic goes down and does not recover until the MXP_MR_10DME card is able to come up. It is not known when or if this issue will be resolved.

CSCsb94736

After a fault condition (trunk LOS or Y-cable switch) an MXP_MR_10DME card might fail to detect the login message and traffic might not start for some minutes (after multiple login trials). This can occur in an N-F configuration with MDS switch and MXP_MR_10DME distance extension on, where test equipment traffic is set to 2G Fibre channel (FC) full bandwidth occupancy and started. Stop traffic or keep bandwidth occupancy below 80% during the login phase to work around this issue. This issue will not be resolved.

CSCsb95918

All GFP related alarms are raised with their active severities on the standby card after a Y-Cable protection switch. When a DWDM card (with GFP support) in a Y-Cable protection group becomes standby as a result of a Y-Cable protection switch, the GFP alarms raised when the card was active retain their severities instead of assuming standby severities. The alarms can be seen in the alarm pane if not suppressed, or in the condition pane if suppressed. This issue will be resolved in a future release.

CSCsc36494

Manual Y cable switches with squelching turned off can cause a Fibre channel link with brocade switches to go down.

This issue can be reproduced as follows:

Step 1 Set up MXP_MR_10DME cards so that they are Y cable protected. Squelching is provisioned to be off. Distance extension is turned on.

Step 2 The path between the working pair of Y cable protected cards, has no distance introduced. But the protect path has a delay of 800 km introduced.

Step 3 Start Fibre channel traffic with brocade switches.

Step 4 Perform user-initiated manual Y cable switches from CTC.

After a few switchovers, the FC link will go down. SIGLOSS and GFP-CSF alarms are seen on the CTC.

Cisco recommends you provision squelching to be on when interworking with brocade switches. If for some reason, squelching must be off with brocade switches, Cisco recommends you use a FORCE command to perform Y cable switches. It is not known when or if this issue will be resolved.

CSCsc55771

When two MXP_MR_10DME cards are interconnected through OC-192/STM-64 cross connects and traffic is up, if you hard reset one of the MXP_MR_10DME cards, the traffic might fail to recover. To recover traffic flow, place the client port in OOS,DSBLD state, delete the PPM then recreate it, and reprovision the port. This issue is resolved in Release 7.2.

CSCsc60472

CTC is not able to discover a TL1 OCHCC circuit provisioned over an ITU-T line card (ITU-T OC48/STM16 and ITU-T OC192/STM64). This issue can occur when, using the TL1 client interface, you create the OCHNC layer that will be used by the OCHCC circuit, then create the OCHCC connections that involve the ITU-T line cards. The result is an OCHNC and two OCHCC partial circuits, instead of an OCHNC and a single OCHCC complete circuit. This issue will not be resolved.

CSCsc14290

LOW communication between two nodes equipped with TXP-MR-10E and AIC-I cards does not work with TXP-MR-10E cards in line termination mode, G.709 enabled, GCC present on the trunk port, and LOW circuits created between the transponders and AIC-I; Cisco recommends that you use EOW instead. This issue will be resolved in a future release.

CSCsc58941

Trunk ports of the TXPP_MR_2.5G and MXPP_MR_2.5G can be in facility and terminal loopback at the same time. this can occur if you provision terminal loopback on the protected trunk port after putting the trunk ports in facility loopback. You can clear this condition by removing loopback provisioning on the trunk ports. This issue will be resolved in Release 8.0.

CSCeh94567

Setting a Terminal loopback on an MXP-2.5G-10G trunk port causes OTUK alarms.

This can occur under the following conditions.

1. Two MXP-2.5G-10G cards are connected via the trunk ports.
2. The client ports are connected to respective STM16 line cards.
3. SDCC is enabled on the client ports and the line cards' STM16 port.
4. A terminal loopback is set on the MXP-2.5G-10G trunk port.

This terminal loopback causes OTUK-LOF and OTUK-IA alarms to be reported on both MXP-2.5G-10G trunk ports. This issue will not be resolved.

CSCef15415

RMON TCAs are not raised on the TXPP_MR_2.5G client port after a hardware reset. To see this issue, provision two nodes with TXPP_MR_2.5G (TXP-1 and TXP-2) as follows.

Step 1 Connect the TXP-1 DWDM-A trunk to the TXP-2 DWDM-A trunk.

Step 2 Connect the TXP-1 DWDM-B trunk to the TXP-2 DWDM-B trunk.

Step 3 Create an external fiber loopback on the TXP-1 client.

Step 4 Connect the TXP-2 client to a traffic generator.

Step 5 Provision 1G FC payload on the TXP-1 and TXP-2.

Step 6 Ensure that traffic is running smoothly.

Step 7 Provision RMON thresholds using TL1 for all TXPP_MR_2.5G ports (client and trunks).

Step 8 Apply a hardware reset to the TXPP_MR_2.5G.

After the card reboots, only DWDM-A and DWDM-B (trunk) port RMON TCAs are raised in the CTC History pane. RMON TCAs for port 1 (client) are not raised. This issue will not be resolved.

CSCef15452

RMON TCAs are not raised when the RMON history is cleared on TXPP_MR_2.5G card. To see this issue, provision two nodes with TXPP_MR_2.5G (TXP-1 and TXP-2) as follows.

Step 1 Connect the TXP-1 DWDM-A trunk to the TXP-2 DWDM-A trunk.

Step 2 Connect the TXP-1 DWDM-B trunk to the TXP-2 DWDM-B trunk.

Step 3 Create an external fiber loopback on the TXP-1 client.

Step 4 Connect the TXP-2 client to a traffic generator.

Step 5 Provision 1G FC payload on the TXP-1 and TXP-2.

Step 6 Ensure that traffic is running smoothly.

Step 7 Provision RMON thresholds using TL1 for all TXPP_MR_2.5G ports (client and trunks).

Step 8 While the traffic is running reset the RMON history by clicking the Clear button in the CTC Payload PM pane.

RMON TCAs are not raised for any port. This issue will not be resolved.

CSCuk48503

Under very specific conditions the MXPD fails the Telcordia GR-253/G.825 Jitter generation mask test on the 10G transmit trunk port. The 2.5 G transmit client jitter generation remains within mask and does not exhibit this issue.

This only occurs when, in SONET mode, with no FEC, no G,709, and client interfaces looped back, with non-synchronous clocking, and performing the following steps.

Step 1 Connect a jitter testbox TX to Trunk RX port.

Step 2 Connect a jitter testbox RX to Trunk TX port.

The jitter testbox TX clock recovers from RX with an additional 5 ppm offset added. This issue will not be resolved.

CSCef50726

Receive client fiber removal can cause a switch from the protect to the active in a TXPP_MR_2.5G. To see this issue, perform the following steps.

Step 1 Set up two nodes with TXPP_MR_2.5G (call the nodes TXP-1 and TXP-2).

Step 2 Ensure that TXP-1 DWDM-A trunk is connected to TXP-2 DWDM-A trunk with a 100 Km span.

Step 3 Ensure that TXP-1 DWDM-B trunk is connected to TXP-2 DWDM-B trunk with a 0 Km span.

Step 4 Ensure that TXP-1 client has an external fiber loopback.

Step 5 Connect the TXP-2 client to a traffic generator.

Step 6 Provision TXP-1 and TXP-2 with FICON 1G payload.

Step 7 Ensure that traffic is running smoothly on the protected span.

Step 8 Remove the receive client fiber at the near end.

This causes the far end trunk to switch from protect to working span. Similarly, removal of the receive Client fiber at far end causes the near end trunk to switch from the protect to the working span. (Note that the traffic is already lost due to the receive client fiber pull.) To work around this issue, manually switch via CTC from the working to the protect span. This issue will not be resolved.

CSCef13304

Incorrect ALS initiation causes a traffic outage on an FC payload. This issue can be seen by performing the following steps.

Step 1 Set up two nodes with TXPP_MR_2.5G (call these nodes TXP-1 and TXP-2).

Step 2 Connect the TXP-1 DWDM-A trunk to the TXP-2 DWDM-A trunk.

Step 3 Connect the TXP-1 DWDM-B trunk to the TXP-2 DWDM-B trunk.

Step 4 Provision the TXP-1 client with an external fiber loopback.

Step 5 Connect the TXP-2 client to a traffic generator.

Step 6 Ensure that TXP-1 and TXP-2 have 1G FC payload provisioned.

Step 7 Enable ALS on TXP-1 trunk port and set it to “Manual Restart.”

Step 8 When traffic is running, remove the receive and transmit fibers on TXP1 port 1 (client). Traffic goes down and shutdown on TXP-1 port 2 (trunk) displays “No.”

Step 9 Reconnect the fibers for TXP-1 port 1 (client).

ALS is now initiated on TXP-1 port 2 (trunk) and the laser shuts down. Traffic never comes back.

Note This issue is restricted to the TXPP_MR_2.5G card.

To recover from this situation, perform a manual restart or disable the ALS in this configuration. This issue will not be resolved.

CSCuk51184

When downloading Release 4.7 nodes with Release 4.6 installed, The 15454-32MUX-O and 15454-32DMX-O report an AWG Temperature fail low alarm that subsequently clears. This also occurs when downgrading from Release 4.7 to Release 4.6, where the AWG Temperature alarm fail is high. This issue cannot be resolved.

CSCec22885

AS-MT is not enabled in Port 3 when a loopback is applied. To see this issue, on the TXPP card, make the following 3 changes before clicking Apply:

Step 1 Change Port 2 to OOS-MT from IS.

Step 2 Change Port 3 to OOS-MT from IS.

Step 3 Change Port 2 to facility or terminal loopback.

Now, when you click Apply, CTC issues the error message: “Error applying changes to row2 peer trunk port must not be IS.” Port 3 is still IS and the loopback changes are not applied. You must place Port 3 in the OOS-MT state, apply the changes, and then change the loopback to recover.

This error occurs only when all three of the above changes are attempted at the same time.

To avoid this issue, first change both the trunk ports to OOS-MT, click Apply, and then place port 2 in loopback and click Apply again. This issue will not be resolved.

CSCed76821

With Y-cable provisioned for MXP-MR-2.5G cards, if you remove the client receive fiber on one side, the far end takes greater than 100 ms to switch away from the affected card. This issue will not be resolved.

CSCef44939

Under certain conditions you may be unable to provision an Express Order Wire (EOW) circuit using an MXP_2.5G_10G or TXP_MR_10G card trunk port. This can occurs as follows.

Step 1 Provision an MXP_2.5G_10G or TXP_MR_10G card within a node.

Step 2 Disable OTN.

Step 3 Provision DCC on both client and trunk ports.

Step 4 Go to the Network view **Provisioning** > **Overhead Circuits** tab.

During the EOW circuit provisioning only the MXP/TXP client ports are listed for the selection. This issue will not be resolved.

CSCuk51185

After a soft reset of an OSCM or OSC-CSM card, a CONTBUS-IO alarm is raised. This issue will not be resolved.

CSCuk50144

Neither E1 nor E2 circuits are available for EOW circuits on TXP_MR_2.5 TXT in Section and Line Termination mode. This issue will not be resolved.

CSCee45443

When the FICON bridge does not receive the expected number of idle frames between data packets it will transition to SERV MODE. This issue will not be resolved.

CSCec40684

After a database restore TXPP trunk ports might report SF, resulting in a traffic outage. The SF occurs when you restore the database and then put the port OOS for DWDM cards; then the operating mode in the database is different from the current operating mode. To avoid this issue, either put the DWDM port OOS before restore the database, or, after restoring the database, reset the DWDM cards. This issue will not be resolved.

CSCec51270

Far end traffic does not switch in line termination mode with .G709 off. This can occur with non-revertive Y-cable, and DCC enabled, under certain specific conditions. To avoid this issue, turn on .G709 when in line mode. This issue will not be resolved.

CSCuk42668

TXP-MR-2.5G F1-UDC may not be passed through in a line-terminated configuration with OTN off. This can occur with clean, OC-3/STM-1, line-terminated traffic, with OTN disabled, when you create a D1-D3 tunnel, a D4-D12 tunnel, and an F1-UDC from client to client. This issue will not be resolved.

CSCuk42752

If you go to the Overhead Circuits Tab in network view and select any User Data, F1 or User Data D4-D12 circuit type, no nXP cards are available for selection in the Endpoints. However, user Data type circuits can still be made end-to-end (where “end-to-end” refers to external cards, such as AIC to AIC) if the nXP cards are put in Transparent mode. This issue will not be resolved.

CSCeb49422

With TXPP cards, a traffic loss up to six seconds can occur during a DWDM protection switch. This behavior may be exhibited during protection switches by certain third-party fiber channel switches due to loss of buffer credits resulting in a reconvergence of the fiber channel link. This issue will not be resolved.

CSCeb53044

The 2G Fiber Channel (FC) payload data type in the TXP_MR_2.5G and TXPP_MR_2.5G cards do not support any 8B/10B Payload PM monitoring. This is as designed.

CSCea78210

The TXP_MR_2.5G and TXPP_MR_2.5G cards do not support TX Optical power performance monitoring on the trunk port. This is as designed.

CSCeb32065

Once engaged, ALR will not restart on the trunk lines of a TXP or TXPP card. This occurs whenever ALR engages on the trunk lines of a TXP or TXPP card and the recover pulse width is provisioned to less than 40 seconds. This is a function of the trunk laser turn-on time, and the limiting recovery pulse width will vary by card. To avoid this issue, provision the pulse width to 40 seconds or more. This issue will not be resolved.

CSCuk42588

With ALS mode configured as “Auto Restart” or “Manual Restart,” it is possible the ALS Pulse Duration Recovery time can be set to values out of ITU-T recommendation G.664. You can use values out of the range defined in ITU-T recommendation G.664 only in order to interoperate with equipment that lasers cannot turn on or off within the required pulse time. To stay within the specification, you can set this value to 2 seconds and up to 2.25 seconds.

CSCea81219

On the TXPP, the default value for Tx Power High for TCAs & Alarms is too high for the trunk ports. Since Tx Power TCA and Alarm are not supported for trunk ports, this caveat is for informational purposes only.

CSCeb27187

During a Y-Cable protection switch, the client interface sends 200,000 to 300,000 8B/10B errors towards the attached Catalyst 3550 switch. The switch reacts to this large amount of 8B/10B errors by reinitializing the interface and spanning tree. The end result is that a protection switch can lead to a 30-45 second traffic hit if the switch is running spanning tree (default mode). This is expected behavior.

CSCea87290

In a Y-Cable protection group, if GCCs are defined on both cards, both cards' active LEDs will be green. This is by design.

CSCeb12609

For the TXPP, attenuating Port 2 Rx signal, SD, and SF alarms are not declared before LOS-P is raised. This is due to the intrinsic design of the optical interface, which allows required BER performances with dispersion and OSNR penalties.

This can occur when Port 2 is in back to back or has low dispersions and high OSNR.

CSCea68773

The ACTV/STBY LED shows AMBER when a 2.5G transponder is first connected. The DWDM cards introduced a new design: When all the ports are OOS on a card, the card is considered to be in standby mode.

Interoperability

CSCds13769: Fujitsu FLM-150 and Nortel OC-3 Express

You cannot provision the FLM-150 and OC-3 Express in 1+1 revertive switching mode. The problem occurs when the ONS 15454 issues a user request in revertive mode to the protect channel. When the user request is cleared, the ONS 15454 issues a No Request. However, the FLM-150 and OC-3 Express issues a Do Not Revert, which causes traffic to remain on the protection channel. Based on Telcordia GR-253, section 5.3.5.5, the FLM-150 and the OC-3 Express should respond with a No Request.

BLSR Functionality

CSCei67965

A VT traffic hit up to 140 ms can occur when an intermediate node of the VT circuit is isolated. For example, if you have three nodes, A, B, and C, where the circuit is routed from A to C via B, when you isolate Node B, Nodes A and C perform STS-level 100 ms squelching as a part of the VT squelching process. However, the timer resolution on the cross connect card yields 16 2/3 ms accuracy, so the 100 ms timer sometimes (about 80% of the time, depending on the number of VT circuits on a ring) expires approximately 17 ms delayed. This causes VT traffic to be squelched for slightly more than 100 ms. Due to system limitation of timer resolution accuracy and task scheduling delay, there is no further optimization available in the current 15454 BLSR design.

CSCed10127

Extra traffic is not restored when an SF-R occurs on the same span where a lockout of protect is applied at the opposite node, and where the extra traffic is sourced, destined, or travels through the node with the SF-R. to work around this, issue a lockout on each end of the span at the node where the SF-R occurs. Extra traffic should then be restored. This issue will not be resolved.

CSCea59342

DS3 PCA traffic may take up to 20 seconds to recover after a BLSR switch is cleared. This can occur with DS3 PCA traffic on two-Fiber or four-Fiber BLSR configuration with XCVT cards in the same nodes as the DS3 cards. This issue will be resolved in a future release.

CSCdw58950

You must lock out protection BLSR, 1+1, and UPSR traffic to avoid long, or double traffic hits before removing an active XCVT or XC10G card. You should also make the active cross connect card standby before removing it.

CSCdv53427

In a two ring, two fiber BLSR configuration (or a two ring BLSR configuration with one two fiber and one four fiber ring) it is possible to provision a circuit that begins on one ring, crosses to a second ring, and returns to the original ring. Such a circuit can have protection vulnerabilities if one of the common nodes is isolated, or if a ring is segmented in such a way that two non-contiguous segments of the circuit on the same ring are each broken.

Database Restore on a BLSR

When restoring the database on a BLSR, follow these steps:

Step 1 To isolate the failed node, issue a force switch toward the failure node from the adjacent east and west nodes.

Step 2 If more than one node has failed, restore the database one node at a time.

Step 3 After the TCC2/TCC2P has reset and booted up, ensure that the “BLSR Multi-Node Table update completed” event has occurred for all nodes in the ring.

Step 4 Release the force switch from each node.

UPSR Functionality

CSCee53579

Traffic hits can occur in an unprotected to UPSR topology upgrade in unidirectional routing. If you create an unprotected circuit, then upgrade the unprotected circuit to a UPSR circuit using Unprotected to UPSR wizard, selecting unidirectional routing in the wizard, the circuit will be upgraded to a UPSR circuit. However, during the conversion, traffic hits on the order of 300 ms should be expected. This issue will not be resolved.

Active Cross Connect (XC10G/XCVT) or TCC2/TCC2P Card Removal

As in BLSR and 1+1, you must perform a lockout on UPSR before removing an active cross connect or TCC2/TCC2P card. The following rules apply to UPSR.

Active cross connect (XC10G/XCVT) cards should not generally be physically removed. If the active cross connect or TCC2/TCC2P card must be removed, you can first perform an XCVT/XC10G side switch or TCC2/TCC2P reset and then remove the card once it is in standby, or you can perform a lockout on all circuits that originate from the node whose active cross connect card or active TCC2/TCC2P will be removed (performing a lockout on all spans will also accomplish the same goal). No lockout is necessary for switches initiated through CTC or through TL1.

Bridge and Roll

CSCsc60635

Bridge and Roll is allowed on the STM1E card, although it is not supported. This issue will be resolved in Release 8.0.

Alarms

CSCsc66474

The ODU-Alarm indication signal is not sent downstream on a client when the line card is provisioned as line terminated. This issue will not be resolved.

SNMP

CSCsc62801

For nodes configured in multishelf mode using the default LAN configuration, SNMP traps are not sent to the management system. To avoid this issue, provision any the DCN-connected node as “Socks proxy,” then, on such nodes add the following static route:

- Destination: 0.0.0.0
- Next hop: DCN Router

- Cost: 10
- Provision any non-DCN connected node as ENE.

A documented solution is available in the February 2006 online version of the *ONS 15454 DWDM Reference Manual*, Release 7.0.

SNMP Attribute Changes

The following SNMP attributes will be replaced in future releases, and will no longer be supported after Release 7.0.

- cMsDwdmIfMultiplexSectionRingDirection
- cMsDwdmIfTransportRingDirection
- cMsDwdmIfChannelRingDirection

TL1

Note To be compatible with TL1 and DNS, all nodes must have valid names. Node names should contain alphanumeric characters or hyphens, but no special characters or spaces.

CSCsb72582

You cannot perform an ENT-EQPT for a valid card type when the current equipment state is OOS-AUMA,MEA&UAS. When the fault PPM comes up as OOS-AUMA,MEA&UAS and then the ENT-EQPT command is entered using TL1, the command is rejected. This issue will be resolved in a future release.

CSCsc41650

Using a TL1 script to rapidly preprovision/delete various cards repeatedly in the same slot will reboot the TCC approximately 1 out of 10 times. Put a delay of about 10 seconds between preprovisioning/deletion cycles and the node will not reboot. This issue will be resolved in a future release.

CSCdu53509

When a TL1 session to a remote node (ENE) is established via a gateway node (GNE) and you have changed the node name of the ENE via either TL1, CTC or SNMP, then you must wait for about 30 seconds to issue a TL1 command via the GNE. This delay is to permit the updates to propagate to all nodes in the network. During this transition, neither the old node name nor the new node name can be used in the TL1 session to access the ENE. This 30 second window may be reduced in a future release.

Resolved Caveats for Release 7.0.x

This section documents caveats resolved in Release 7.0.x.

Maintenance and Administration

CSCsd67191

A node might rarely report DCC failure and loses all connections when it is participating in a large network with several host routes, where multiple netJobAdd calls are likely, which eventually deplete the allowable ring buffer. When the MCC driver fails to complete the add it stops responding to receive packets and the DCC fails. Proper subnetting and OSPF summarizing will avoid excessive host routes, reducing the chance for such a scenario. This issue is resolved in Releases 6.2, 7.0.2, 7.2, and 8.0.

CSCei67897

Rarely, autoprovisioned audits (those with the unique ID of 0) can become stranded after a bulk roll of VC LO circuits prior to deletion of those circuits. If an attempt was made previously to delete all such circuits, you can use subtractive logic to discover which circuits have become stranded. That is, matrices indicating usage in the node view, Maintenance > Cross-connect > Resource Usage window will indicate stranded circuits.

Once you have identified that there are stuck STSs, go to the card view for each affected trunk card and view the Maintenance > Loopback > SONET STS tabs. From here you can view all used STSs, including any stuck STSs. Determine which STSs in your network have no circuit associated with them, then create and subsequently delete a LO circuit on each affected STS. This will clean up the stuck STSs. This issue is resolved in Release 7.0.

CSCsb44920

The error message ('null') is invalid when, in a failed merge operation on two portless circuits, one circuit loses its connection after the merge. You can see this if you merge two portless intranode UPSR circuits, where one circuit has one source and two drops, and the other circuit has two sources and one drop. Though the two drops of the first circuit might be aligned with the two drops of the second circuit, all of them are inside one physical link (not a valid UPSR topology). To recover from this situation, open a new CTC session. This will return the circuits to their status prior to the failed merge. This issue is resolved in Release 7.0.

CSCuk52850

In a fiber cut scenario on the LINE-RX, with OSC and channels provisioned, transient LOS-P or LOS-O alarms might be raised. This issue is resolved in Release 7.0.

Electrical IO Cards

CSCsb48303

The DS-1 line state of the portless ports (13, 14 and greater) does not match the corresponding DS-3 line state when a DS3XM-12 conversion circuit is provisioned with the IS drop port state.

To see this, create a 1-way DS3XM-12 conversion circuit with the drop port state set to IS. Delete the conversion circuit, leaving the IS port state. Note that the DS-1 line state will now be OOS by design. If there is no circuit, DS-1 portless port lines will be placed in OOS state.

Create the DS3XM-12 conversion circuit again as before. The DS-1 portless port lines do not transition to IS.

To recover from this issue, change the DS-3 port state to OOS_MT and then to IS. The DS-1 portless port lines will transition properly. This issue is resolved in Release 7.0.

Data IO Cards

CSCin96350

If L2 protocol tunneling is disabled on an interface when it is not a member of a bridgegroup, this can cause the CAM programming of STP MAC addresses to be incorrect. The spanning tree received on a node is not passed on to the host, and the spanning tree process might not converge due to the STP packets failing to reach the host. If this occurs, add the affected interface to a bridgegroup and disable protocol tunneling. This issue is resolved in Release 7.0.

CSCsb40206

In Asymmetric configuration, with autonegotiation enabled and flow control selected, an ML-series card might fail to synchronize with, or to recognize the asymmetric flow control. This issue is resolved in Release 7.0.

CSCeg15044

IOS does not allow telnet connections when there are simultaneous Telnet requests, even though there might be unused tty lines available. If this issue occurs, a “No Free TTYs error” message is displayed. This issue is resolved in Release 7.0 (and 6.0).

DWDM Cards

CSCsc54518

The OPT-BST amplifier card is in a LASER OFF state, even if input power is provided to all input ports. This issue only occurs with Release 7.0 and can be reproduced on a card with the amplifier turned on, in operating conditions (with lasers on) as follows.

Step 1 From the card-level **Maintenance** tab set ALS Mode to **Manual Restart** and click **Apply**.

Step 2 Set **OSRI** to **ON** and click **Apply**. The amplifier turns off.

Step 3 Set **OSRI** to **OFF** and click **Apply**. The amplifier stays turned off (this is expected, since in Manual Restart the lasers are turned back on by means of a Request Laser Restart command issued in CTC).

Step 4 Select the **Request Laser Restart** check box in the **Maintenance** tab and click **Apply**.

The amplifier goes into APR for 9 seconds (correct), but after this it turns off; it should go into LASER ON state (State 4 at module level). If this issue occurs, change the card from manual restart to auto restart, then toggle OSRI ON and OFF. This issue is resolved in Release 7.0.2.

CSCsc62581

A T-TX-PWR-MIN TCA is raised and a wrong receive optical power value (of -40 dB) is displayed after a card is reset. The alert and incorrect Rx value both clear in the next 15 min sample period. This issue is resolved in Release 7.0.1.

CSCei37691

The trunk port service state for the TXPP and TXP cards does not transition to OOS-AU,FLT in the presence of an LOS-P alarm. This can occur when the payload signal for LOS-P is missing for the particular port type. This issue is resolved in Release 7.0.

CSCuk57046

An unexpected Mismatch Equipment Attributes (MEA) transient alarm can occur on rapidly inserting and removing a PPM. This issue can occur with a TXP_MR_10E-L for which you preprovision an OC-192 PPM. The transient alarm is raised on the PPM. This issue is resolved in Release 7.0.

Alarms

CSCei37745

When VT and STS level alarms are raised at the same time, the VT level alarm is not demoted or promoted in correlation with other VT or STS level alarms. This issue is resolved in Release 7.0.

BLSR Functionality

CSCct03919

VT1.5 and VC3/VC12 squelching is not supported in BLSR/MS-SPRing. This issue is resolved in Release 7.0.

CSCeh90643

Before secondary node isolation in a scenario where DRI PCA traffic is provisioned on a protect channel corresponding to a working channel for active DRI protected traffic, with the secondary node of the DRI PCA configured as the primary node of the protected DRI traffic, and the primary node of the DRI PCA configured as the secondary node of the protected DRI traffic, you must perform a user service selector switch command on DRI protected traffic on the secondary node for DRI PCA traffic (primary node for DRI protected traffic). Failing to issue the switch could result in loss of DRI protected traffic during the secondary node isolation. This issue is resolved in Release 7.0.

Bridge and Roll

CSCei37364

When a rollTo leg is not receiving a good signal, and because of this the rollPending alarm is not cleared, there is no alarm indicating the reason that the RollPending alarm fails to clear. This issue is resolved in Release 7.0.

TL1

CSCsc62784

The Calibration Tilt is not properly changed using the TL1 interface. The reference tilt is changed instead. This issue can be seen when you try to change the CALTILT parameter on amplifier cards using the ED-OTS command. To avoid this issue, use CTC. This issue is resolved in Release 7.0.1.

New Features and Functionality

This section highlights new features and functionality for Release 7.0.x. For detailed documentation of each of these features, consult the user documentation.

New Features for Release 7.0.2

The following feature has been added for Release 7.0.2.

Daylight Savings Time Support

With Release 7.0.2 CTC and TL1 display daylight savings time (DST) in keeping with the new DST rules applicable from 2007 forward. As described in the change in energy policy for the United States of America (USA), the DST start date will be the 2nd Sunday of March and the DST end date will be 1st Sunday of November.

The following features were added for Release 7.0.

New Hardware

MXP_MR_10DME-C and MXP_MR_10DME-L Multirate Muxponder Cards

The 10-Gbps Multirate Muxponder-100 GHz-Tunable 15xx.xx-15yy.yy C-band and L-band (MXP_MR_10DME-C and MXP_MR_10DME-L) cards aggregate a mix of client Storage Area Network (SAN) service client inputs (GE, FICON, and Fibre Channel) into one 10-Gbps STM-64/OC-192 DWDM signal on the trunk side. They provide one long-reach STM-64/OC-192 port per card and are compliant with Telcordia GR-253-CORE and ITU-T G.957.

The cards support aggregation of the following signal types:

- 1-Gigabit Fibre Channel
- 2-Gigabit Fibre Channel
- 4-Gigabit Fibre Channel
- IBM FICON-1G
- IBM FICON-2G
- 1-Gigabit Ethernet
- 1-Gigabit ISC-Compatible (ISC-1)
- 1-Gigabit ISC-Peer (ISC-3)
- 2-Gigabit ISC-Peer (ISC-3)

The MXP_MR_10DME-C and MXP_MR_10DME-L muxponders pass all SONET/SDH overhead bytes transparently.

The digital wrapper function (ITU-T G.709 compliant) formats the DWDM wavelength so that it can be used to set up GCCs for data communications, enable FEC, or facilitate performance monitoring. The MXP_MR_10DME-C and MXP_MR_10DME-L cards work with OTN devices defined in ITU-T G.709. The cards support G.709 OTU2 digital wrapper, an industry standard method for asynchronously mapping a SONET/SDH payload into a digitally wrapped envelope. Aggregation of input service signals is provided at the SONET level via GFP-T in STS24c or STS48c framing (depending on the service type).

Note Because the client payload cannot oversubscribe the trunk, a mix of client signals can be accepted, up to a maximum limit of 10 Gbps.

You can install MXP_MR_10DME-C and MXP_MR_10DME-L cards in Slots 1 to 6 and 12 to 17.

Note The MXP_MR_10DME-C and MXP_MR_10DME-L cards are not compatible with the MXP_2.5G_10G card, which does not support full optical transparency.

The MXP_MR_10DME-C card features a tunable 1550-nm C-band laser on the trunk port. The laser is tunable across 82 wavelengths on the ITU grid with 50-GHz spacing between wavelengths. The MXP_MR_10DME_L features a tunable 1580-nm L-band laser on the trunk port. The laser is tunable across 80 wavelengths on the ITU grid, also with 50-GHz spacing. Each card features four 1310-nm lasers on the client ports and contains five transmit and receive connector pairs (labeled) on the card faceplate. The cards use dual LC connectors on the trunk side and use SFP modules on the client side for optical cable termination. The SFP pluggable modules are SX multimode or LX single-mode interface and support an LC fiber connector.

Details regarding the input data rate, encapsulation method, and data rates available for each client interface can be found in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

A buffer-to-buffer credit management scheme provides FC flow control. With this feature enabled, a port indicates the number of frames that can be sent to it (its buffer credit), before the sender is required to stop transmitting and wait for the receipt of a “ready” indication The MXP_MR_10DME-C and MXP_MR_10DME-L cards support FC credit-based flow control with a buffer-to-buffer credit extension of up to 1600 km for 1G FC. up to 800 km for 2G FC, or up to 400km for 4G FC. The feature can be enabled or disabled.

The MXP_MR_10DME-C and MXP_MR_10DME-L cards feature a 1550-nm laser for the trunk/line port and a 1310-nm or 850-nm laser (depending on the SFP) for the client ports. The cards contain eight 12.5 degree downward tilt SFP modules for the client interfaces. For optical termination, each SFP uses two LC connectors, which are labeled TX and RX on the faceplate. The trunk port is a dual-LC connector with a 45 degree downward angle.

Key Features

The MXP_MR_10DME-C and MXP_MR_10DME-L cards have the following high level features:

- Onboard E-FEC processor—The processor supports both standard RS (specified in ITU-T G.709) and E-FEC, which allows an improved gain on trunk interfaces with a resultant extension of the transmission range on these interfaces. The E-FEC functionality increases the correction capability of the transponder to improve performance, allowing operation at a lower OSNR compared to the standard RS (237,255) correction algorithm. A new BCH algorithm implemented in E-FEC allows recovery of an input BER up to 1E-3.
- Pluggable client interface optic modules—The MXP_MR_10DME-C and MXP_MR_10DME-L cards have modular interfaces. Two types of optics modules can be plugged into the card. These include an OC-48/STM 16 SR-1 interface with a 7 km nominal range (for short range and intra-office applications) and an IR-1 interface with a range up to 40 km. SR-1 is defined in Telcordia GR-253-CORE and in I-16 (ITU-T G.957). IR-1 is defined in Telcordia GR-253-CORE and in S-16-1 (ITU-T G.957).
- Y-cable protection—Supports y-cable protection between the same card type only, on ports with the same port number and signal rate.
- High level provisioning support—The cards are initially provisioned using Cisco MetroPlanner software. Subsequently, the card can be monitored and provisioned using CTC software.
- Automatic laser shutdown (ALS), a safety mechanism used in the event of a fiber cut.
- Link monitoring and management—The cards can use either G.709 or SONET OC-192 overhead bytes to monitor and manage incoming trunk interfaces.
- Automatic timing source synchronization—The MXP_MR_10DME-C and MXP_MR_10DME-L cards normally synchronize from the TCC2/TCC2P card. If for some reason, such as maintenance or upgrade activity, the TCC2/TCC2P is not available, the cards automatically synchronize to one of the input client interface clocks.
- Configurable squelching policy—The cards can be configured to squelch the client interface output if there is LOS at the DWDM receiver or if there is a remote fault. In the event of a remote fault, the card can either squelch the laser or send an error code order set.
- The cards are tunable across the full C band (MXP_MR_10DME-C) or full L band (MXP_MR_10DME-L), thus eliminating the need to use different versions of each card to provide tunability across specific wavelengths in a band. For the specific wavelengths for each band, see the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

TXP_MR_10E_C and TXP_MR_10E_L Multirate Transponder Cards

The 10-Gbps Transponder-100-GHz-Tunable (TXP_MR_10E_C and TXP_MR_10E_L) cards are multirate transponders for the ONS 15454 platform. They processes one 10-Gbps signal (client side) into one 10-Gbps, 100-GHz DWDM signal (trunk side). The TXP_MR_10E_C is tunable over the entire set of C-band wavelength channels (82 channels spaced at 50 GHz on the ITU grid). The TXP_MR_10E_L is tunable over the entire set of L-band wavelength channels (80 channels spaced at 50 GHz on the ITU grid) and is particularly well suited for use in networks that employ dispersion shifted (DS) fiber or SMF-28 single-mode fiber.

The advantage of these cards over previous versions (TXP_MR_10G and TXP_MR_10E) is that there is only one version of each card (one C-band version and one L-band version) instead of several versions needed to cover each band.

You can install TXP_MR_10E_C and TXP_MR_10E_L cards in Slots 1 to 6 and 12 to 17 and provision the cards in a linear configuration, BLSR/MS-SPRing, UPSR/SNCP, or a regenerator. The cards can be used in the middle of BLSR/MS-SPRing or 1+1 spans when the cards are configured for transparent termination mode.

The TXP_MR_10E card features a universal transponder 2 (UT2) 1550-nm tunable laser (C band) or a UT2 1580-nm tunable laser (L band) for the trunk port and a separately orderable ONS-XC-10G-S1 1310-nm laser XFP module for the client port. On its faceplate, the TXP_MR_10E_C and TXP_MR_10E_L cards contain two transmit and receive connector pairs, one for the trunk port and one for the client port. Each connector pair is labeled.

Key Features

The key features of the TXP_MR_10E_C and TXP_MR_10E_L cards are:

- A tri-rate client interface (available through the ONS-XC-10G-S1 XFP, ordered separately):
  - OC-192 (SR1)
  - 10GE (10GBASE-LR)
  - 10G-FC (1200-SM-LL-L)
- A UT2 module tunable through the entire C band (TXP_MR_10E_C card) or L band (TXP_MR_10E_L card). The channels are spaced at 50 GHz on the ITU grid.
- OC-192 to ITU-T G.709 OTU2 provisionable synchronous and asynchronous mapping

Client Interface

The client interface is implemented with a separately orderable XFP module. The module is a tri-rate transceiver, providing a single port that can be configured in the field to support an OC-192 SR-1 (Telcordia GR-253-CORE) or STM-64 I-64.1 (ITU-T G.691) optical interface, as well as 10GE LAN PHY (10GBASE-LR), 10GE WAN PHY (10GBASE-LW), or 10G FC signals.

The client side XFP pluggable module supports LC connectors and is equipped with a 1310-nm laser.

DWDM Trunk Interface

On the trunk side, the TXP_MR_10E_C and TXP_MR_10E_L cards provide a 10-Gbps STM-64/OC-192 interface. There are 80 tunable channels available in the 1550-nm C band or 82 tunable channels available in the 1580-nm L band on the 50-GHz ITU grid for the DWDM interface.

The TXP_MR_10E_C and TXP_MR_10E_C cards provide 3R transponder functionality for this 10-Gbps trunk interface. Therefore, the card is suited for use in long-range amplified systems. The DWDM interface is compliant with ITU-T G.707, ITU-T G.709, and Telcordia GR-253-CORE standards.

The DWDM trunk port operates at a rate that is dependent on the input signal and the presence or absence of the ITU-T G.709 Digital Wrapper/FEC. The possible trunk rates are:

- OC192 (9.95328 Gbps)
- OTU2 (10.70923 Gbps)
- 10GE (10.3125 Gbps) or 10GE into OTU2 (nonstandard 10.0957 Gbps)
- 10G FC (10.51875 Gbps) or 10G FC into OTU2 (nonstandard 11.31764 Gbps).

The maximum system reach in filterless applications without the use of optical amplification or regenerators is nominally rated at 23 dB over C-SMF fiber. This rating is not a product specification, but is given for informational purposes. It is subject to change.

Y-Cable Protection

The TXP_MR_10E card supports Y-cable protection, which provides transponder equipment protection without client terminal equipment interface protection. A single client interface can be split between two transponder cards using a Y-protection device.

With Y-cable protection, two TXP_MR_10E_C or two TXP_MR_10E_L transponder cards can be joined in a Y-cable protection group. In Y-cable protection, the client ports of the two cards are joined by Y cables. An incoming client signal is injected into the Rx Y-cable port and is split between the two cards (connected to Rx client ports) in the protection group. The Tx client signals from the two protection group cards are connected to the correspondent ports of the Tx Y cable. Only the Tx client port of the active card is turned on and transmits the signal towards the receiving client equipment.

If you create a GCC using a digital wrapper and apply it to either card of the Y-cable protect group, the DWDM trunk (span) port stays permanently active, regardless of the switch state. When you provision a GCC, you are provisioning unprotected overhead (OH) bytes. The GCC is not protected by the protection group.

Enhanced FEC Feature

A key feature of the TXP_MR_10E_C and TXP_MR_10E_L cards is the availability to configure the forward error correction in three modes: NO FEC, FEC, and Enhanced FEC (E-FEC). The output bit rate is always 10.7092 Gbps as defined in ITU-T G.709, but the error coding performance can be provisioned as follows:

- NO FEC—No forward error correction
- FEC—Standard ITU-T G.975 Reed-Solomon algorithm
- E-FEC—Standard ITU-T G.975.1 algorithm, which is a super FEC code.

FEC and E-FEC Modes

As client side traffic passes through the TXP_MR_10E_C and TXP_MR_10E_L cards, it can be digitally wrapped using FEC mode, E-FEC mode, or no error correction at all. The FEC mode setting provides a lower level of error detection and correction than the E-FEC mode setting of the card. As a result, using E-FEC mode allows higher sensitivity (lower OSNR) with a lower bit error rate than FEC mode. E-FEC enables longer distance trunk-side transmission than with FEC.

The E-FEC feature is one of three basic modes of FEC operation. FEC can be turned off, FEC can be turned on, or E-FEC can be turned on to provide greater range and lower BER. The default mode is FEC on and E-FEC off. E-FEC is provisioned using CTC.

Because the transponder has no visibility into the data payload and detect circuits, the TXP_MR_10E_C and TXP_MR_10E_L cards do not display circuits under the card view.

Client-to-Trunk Mapping

The TXP_MR_10E_C and TXP_MR_10E_L cards can perform ODU2-to-OCh mapping, which allows operators to provision data payloads in a standard way across 10-Gbps optical links.

Digital wrappers that define client side interfaces are called Optical Data Channel Unit 2 (ODU2) entities in ITU-T G.709. Digital wrappers that define trunk side interfaces are called Optical Channels (OCh) in ITU-T G.709. ODU2 digital wrappers can include Generalized Multiprotocol Label Switching (G-MPLS) signaling extensions to ITU-T G.709 (such as Least Significant Part [LSP] and Generalized Payload Identifier [G-PID] values) to define client interfaces and payload protocols.

Automatic Laser Shutdown

The ALS procedure is supported on both client and trunk interfaces. On the client interface, ALS is compliant with ITU-T G.664 (6/99). On the data application and trunk interface, the switch on and off pulse duration is greater than 60 seconds. The on and off pulse duration is user-configurable.

MXP_2.5G_10E_C and MXP_2.5G_10E_L Cards

The 2.5-Gbps-10-Gbps Muxponder-100 GHz-Tunable (MXP_2.5G_10E_C and MXP_2.5G_10E_L) cards are DWDM muxponders for the ONS 15454 platform that support full optical transparency on the client side. The cards multiplex four 2.5 Gbps client signals (4 x OC48/STM-16 SFP) into a single 10-Gbps DWDM optical signal on the trunk side. The MXP_2.5G_10E_C and MXP_2.5G_10E_L cards provide wavelength transmission service for the four incoming 2.5 Gbps client interfaces. The MXP_2.5G_10E_C and MXP_2.5G_10E_L muxponders pass all SONET/SDH overhead bytes transparently.

The digital wrapper function (ITU-T G.709 compliant) formats the DWDM wavelength so that it can be used to set up GCCs for data communications, enable FEC, or facilitate performance monitoring.

The MXP_2.5G_10E_C and MXP_2.5G_10E_L cards work with OTN devices defined in ITU-T G.709. The cards support ODU1 to OTU2 multiplexing, an industry standard method for asynchronously mapping a SONET/SDH payload into a digitally wrapped envelope.

The MXP_2.5G_10E_C and MXP_2.5G_10E_L cards are not compatible with the MXP_2.5G_10G card, which does not support full optical transparency.

You can install MXP_2.5G_10E_C and MXP_2.5G_10E_L cards in Slots 1 to 6 and 12 to 17. You can provision a card in a linear configuration, as a BLSR/MS-SPRing, a UPSR/SNCP, or a regenerator. The cards can be used in the middle of BLSR/MS-SPRing or 1+1 spans when the cards are configured for transparent termination mode.

The MXP_2.5G_10E_C card features a tunable 1550-nm C-band laser on the trunk port. The laser is tunable across 82 wavelengths on the ITU grid with 50-GHz spacing between wavelengths. The MXP_2.5G_10E_L features a tunable 1580-nm L-band laser on the trunk port. The laser is tunable across 80 wavelengths on the ITU grid, also with 50-GHz spacing. Each card features four 1310-nm lasers on the client ports and contains five transmit and receive connector pairs (labeled) on the card faceplate. The cards uses dual LC connectors on the trunk side and use SFP modules on the client side for optical cable termination. The SFP pluggable modules are short reach (SR) or intermediate reach (IR) and support an LC fiber connector.

Key Features

The MXP_2.5G_10E_C and MXP_2.5G_10E_L cards have the following high level features:

- Four 2.5 Gbps client interfaces (OC-48/STM-16).
- One 10 Gbps trunk interface.
- The four OC-48 signals are mapped into a ITU-T G.709 OTU2 signal using standard ITU-T G.709 multiplexing.

- Onboard E-FEC processor—The processor supports both standard RS (specified in ITU-T G.709) and E-FEC, which allows an improved gain on trunk interfaces with a resultant extension of the transmission range on these interfaces. The E-FEC functionality increases the correction capability of the transponder to improve performance, allowing operation at a lower OSNR compared to the standard RS (237,255) correction algorithm. A new BCH algorithm implemented in E-FEC allows recovery of an input BER up to 1E-3.
- Pluggable client interface optic modules—The MXP_MP_10E_C and MXP_MP_10E_L cards have modular interfaces. Two types of optics modules can be plugged into the card. These include an OC-48/STM 16 SR-1 interface with a 7 km nominal range (for short range and intra-office applications) and an IR-1 interface with a range up to 40 km. SR-1 is defined in Telcordia GR-253-CORE and in I-16 (ITU-T G.957). IR-1 is defined in Telcordia GR-253-CORE and in S-16-1 (ITU-T G.957).
- High level provisioning support—The cards are initially provisioned using Cisco MetroPlanner software. Subsequently, the card can be monitored and provisioned using CTC software.
- Link monitoring and management—The cards use standard OC-48 OH (overhead) bytes to monitor and manage incoming interfaces. The cards pass the incoming SDH/SONET data stream and its overhead bytes transparently.
- Control of layered SONET/SDH transport overhead—The cards are provisionable to terminate regenerator section overhead. This is used to eliminate forwarding of unneeded layer overhead. It can help reduce the number of alarms and help isolate faults in the network.
- Automatic timing source synchronization—The MXP_MP_10E_C and MXP_MP_10E_L cards normally synchronize from the TCC2/TCC2P card. If for some reason, such as maintenance or upgrade activity, the TCC2/TCC2P is not available, the cards automatically synchronize to one of the input client interface clocks.
- Configurable squelching policy—The cards can be configured to squelch the client interface output if there is LOS at the DWDM receiver or if there is a remote fault. In the event of a remote fault, the card manages multiplex section alarm indication signal (MS-AIS) insertion.
- Full tunablility across the band—The cards are tunable across the full C band (MXP_2.5G_10E_C) or full L band (MXP_MP_10E_L), thus eliminating the need to use different versions of each card to provide tunability across specific wavelengths in a band.

Client Interfaces

The MXP_2.5G_10E_C and MXP_2.5G_10E_C cards provide four intermediate- or short-range OC-48/STM-16 ports per card on the client side. Both SR-1 or IR-1 optics can be supported and the ports use SFP connectors. The client interfaces use four wavelengths in the 1310-nm, ITU 100-MHz-spaced, channel grid.

DWDM Interface

The MXP_2.5G_10E_C and MXP_2.5G_10E_L cards serve as OTN multiplexers, transparently mapping four OC-48 channels asynchronously to ODU1 into one 10-Gbps trunk. The DWDM trunk is tunable for transmission over the entire C band (MXP_2.5G_10E_C) or over the entire L band (MXP_2.5G_10E_L) on the ITU 50-GHz spaced channel grid.

Multiplexing Function

The muxponder is an integral part of the optically transparent ROADM network in which data payload channels and wavelengths are processed exclusively at the optical level without electrical to optical (E-O) conversion. The key function of the MXP_MP_10E_C and MXP_MP_10E_L cards is to multiplex 4 OC-48/STM16 signals onto one ITU-T G.709 OTU2 optical signal (DWDM transmission). The multiplexing mechanism allows the signal to be terminated at a far-end node by another similar card.

Optical transparency on the muxponder is configured using OTUx and ODUx OH bytes. The ITU-T G.709 specification defines OH byte formats that are used to configure, set, and monitor frame alignment, FEC mode, section monitoring, tandem connection monitoring, and optical transparency.

The MXP_2.5G_10E and MXP_MP_10E_L cards perform ODU to OTU multiplexing as defined in ITU-T G.709. The ODU is the framing structure and byte definition (ITU-T G.709 digital wrapper) used to define the data payload coming into one of the SONET/SDH client interfaces on the cards. The term ODU1 refers to an ODU that operates at 2.5-Gbps line rate. On the cards, there are four client interfaces that can be defined using ODU1 framing structure and format by asserting a ITU-T G.709 digital wrapper.

The output of the muxponder is a single 10-Gbps DWDM trunk interface defined using OTU2. It is within the OTU2 framing structure that FEC or E-FEC information is appended to enable error checking and correction.

The MXP_2.5G_10E_C and MXP_2.5G_10E_L cards are synchronized to the TCC2/TCC2P clock during normal conditions and transmits the ITU-T G.709 frame using this clock.

The cards support Y-cable protection. Two cards can be joined in a Y-cable protection group with one card assigned as the working card and the other defined as the protection card. This protection mechanism provides redundant bidirectional paths.

You can configure the Forward Error correction for the cards in three modes: NO FEC, FEC, and E-FEC. So, as client side traffic passes through the MXP_2.5G_10E_C or MXP_2.5G_10E_L card, it can be digitally wrapped using FEC mode error correction or E-FEC mode error correction (or no error correction at all).

For further card details, specifications, and functionality, see the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

New MXP_MR_2.5G and MXPP_MR_2.5G Muxponder Cards

The 2.5-Gbps Multirate Muxponder-100 GHz-Tunable 15xx.xx-15yy.yy (MXP_MR_2.5G) card aggregates a mix and match of client Storage Area Network (SAN) service client inputs (GE, FICON, Fibre Channel, and ESCON) into one 2.5 Gbps STM-16/OC-48 DWDM signal on the trunk side. It provides one long-reach STM-16/OC-48 port per card and is compliant with Telcordia GR-253-CORE.

Note In Release 7.0.x, two additional operating modes are available: pure ESCON (all 8 ports running ESCON), and Mixed mode (port 1 running FC/GE/FICON, and ports 5 through 8 running ESCON). When the card is part of a node running Release 6.0 or below, only one operating mode, FC_GE mode, is available for use.

The 2.5-Gbps Multirate Muxponder-Protected-100 GHz-Tunable 15xx.xx-15yy.yy (MXPP_MR_2.5G) card aggregates various client SAN service client inputs (GE, FICON, Fibre Channel, and ESCON) into one 2.5 Gbps STM-16/OC-48 DWDM signal on the trunk side. It provides two long-reach STM-16/OC-48 ports per card and is compliant with ITU-T G.957 and Telcordia GR-253-CORE.

Because the cards are tunable to one of four adjacent grid channels on a 100-GHz spacing, each card is available in eight versions, with 15xx.xx representing the first wavelength and 15yy.yy representing the last wavelength of the four available on the board. In total, 32 DWDM wavelengths are covered in accordance with the ITU-T 100-GHz grid standard, G.692, and Telcordia GR-2918-CORE, Issue 2. The card versions and their corresponding wavelengths are documented in the Cisco ONS 15454 DWDM Installation and Operations Guide.

Client Interface

The client interface supports the following payload types:

- 2G FC
- 1G FC
- 2G FICON
- 1G FICON
- GE
- ESCON

Note Because the client payload cannot oversubscribe the trunk, a mix of client signals can be accepted, up to a maximum limit of 2.5 Gbps.

Details on the input data rate for each client interface, the encapsulation method, and the mix and match of client interfaces on various ports can be found in the Cisco ONS 15454 DWDM Installation and Operations Guide.

For the MXP_MR_2.5G card, protection is done using Y-cable protection. Two MXP_MR_2.5G cards can be joined in a Y-cable protection group, which provides protection against failures both on the fiber and in the muxponders.

For the MXPP_MR_2.5G card, protection is done using splitter protection, which provides protection against failures due to fiber cuts or unacceptable signal degradation on the trunk side.

Note Switching is performed only if the protect line is error free.

GFP-T performance monitoring (GFP-T PM) is available via remote monitoring (RMON), and trunk PM is managed according to Telcordia GR-253-CORE and ITU G.783/826. Client PM is achieved through RMON for FC and GE.

A buffer-to-buffer credit management scheme provides FC flow control. With this feature enabled, a port indicates the number of frames that can be sent to it (its buffer credit), before the sender is required to stop transmitting and wait for the receipt of a “ready” indication The MXP_MR_2.5G and MXPP_MR_2.5 cards support FC credit-based flow control with a buffer-to-buffer credit extension of up to 1600 km for 1G FC and up to 800 km for 2G FC. The feature can be enabled or disabled.

You can install MXP_MR_2.5G and MXPP_MR_2.5G cards in Slots 1 to 6 and 12 to 17. The TCC2/TCC2P card is the only other card required to be used with these muxponder cards. Cross-connect cards do not affect the operation of the muxponder cards.

The MXP_MR_2.5G card features a 1550-nm laser for the trunk/line port and a 1310-nm or 850-nm laser (depending on the SFP) for the client ports. The card contains eight 12.5 degree downward tilt SFP modules for the client interfaces. For optical termination, each SFP uses two LC connectors, which are labeled TX and RX on the faceplate. The trunk port is a dual-LC connector with a 45 degree downward angle.

The MXPP_MR_2.5G card features a 1550-nm laser for the trunk/line port and a 1310-nm or 850-nm laser (depending on the SFP) for the client port. The card contains eight 12.5 degree downward tilt SFP modules for the client interfaces. For optical termination, each SFP uses two LC connectors, which are labeled TX and RX on the faceplate. There are two trunk port connectors (one for working and one for protect). Each is a dual-LC connector with a 45-degree downward angle.

Automatic Laser Shutdown

The ALS procedure is supported on both client and trunk interfaces. On the client interface, ALS is compliant with ITU-T G.664 (6/99). On the data application and trunk interface, the switch on and off pulse duration is greater than 60 seconds. The on and off pulse duration is user-configurable.

OPT-BST-L Optical Booster Card

The Optical Booster L-Band (OPT-BST-L) has a standard gain range of 8 to 20 dB in the controllable gain tilt mode, and 20 to 27 dB in the uncontrolled gain tilt mode. The OPT-BST-L is designed to support 64 channels at 50-GHz channel spacing, but currently is limited to 32 channels at 100-GHz spacing. The OPT-BST-L is an L-band DWDM EDFA with OSC add-and-drop capability. The card is particularly well suited for use in networks that employ dispersion shifted (DS) fiber or SMF-28 single-mode fiber.

When an ONS 15454 has an OPT-BST-L installed, it is only necessary to have the OSCM to process the OSC. You can install the OPT-BST-L in Slots 1 to 6 and 12 to 17. To control the gain tilt, the OPT-BST-L is equipped with a built-in VOA.

Key Features

The OPT-BST-L features include:

- Fixed gain mode (with programmable tilt)
- True variable gain
- Fast transient suppression
- Nondistorting low-frequency transfer function
- Settable maximum output power
- Fixed output power mode (mode used during provisioning)
- ASE compensation in fixed gain mode
- Full monitoring and alarm handling with settable thresholds
- OSRI, which is a software feature capable (through CTC) of shutting down the optical output power or reducing the power to a safe level (automatic power reduction)
- ALS, which is a safety mechanism used in the event of a fiber cut

Note The optical splitters each have a ratio of 1:99. The result is that the power at the MON TX and MON RX ports is about 20 dB lower than the power at the COM TX and COM RX ports.

Several photodiodes monitor the power for the OPT-BST-L card. The returned power level values are calibrated to the ports on the card. See the Cisco ONS 15454 DWDM Installation and Operations Guide for details.

OPT-AMP-L Preamplifier Card

The OPT-AMP-L is an L-band DWDM optical amplifier module consisting of a two-stage EDFA with mid-stage access loss (MSL) for an external DCU and OSC add-and-drop capability. The card is provisionable in CTC as a preamplifier or booster amplifier and is well suited for use in networks that employ DS fiber or SMF-28 single-mode fiber. The amplifier can operate up to 64 optical transmission channels at a channel spacing of 50 GHz in the wavelength range from 1570 nm to 1605 nm.

The OPT-AMP-L is able to achieve a maximum signal power of 20 dBm throughout the gain and MSL ranges. The amplifier has a variable gain range that is settable from 12 to 24 dBm in the standard gain range and from 24 dBm to 35 dBm with uncontrolled gain tilt. It also provides up to 12 dBm MSL for an external DCU.

When an ONS 15454 has an OPT-AMP-L installed, it is only necessary to have the OSCM to process the OSC. You can install the two-slot OPT-AMP-L in Slots 1 to 6 and 12 to 17. To control the gain tilt, the OPT-AMP-L is equipped with a built-in VOA.

Key Features

The OPT-AMP-L has the following features:

- Maximum power output of 20 dBm
- True variable gain amplifier
- Fast transient suppression; able to adjust power levels in hundreds of microseconds to avoid bit errors in failure or capacity growth situations
- Nondistorting low frequency transfer function
- Mid-stage access loss for dispersion compensation unit
- Constant pump current mode (test mode)
- Constant output power mode (used during optical node setup)
- Constant gain mode.
- Internal ASE compensation in Constant Gain and in Constant Output Power mode
- Programmable tilt
- Full monitoring and alarm handling capability
- Optical safety support through signal loss detection and alarm at any input port, fast power down control (less than one second), and reduced maximum output power in safe power mode

Several photodiodes monitor the power for the OPT-AMP-L card. The returned power level values are calibrated to the card ports. See the *Cisco ONS 15454 DWDM Installation and Operations Guide* for details.

32WSS-L Wavelength Selective Switch Card

The 32-Channel Wavelength Selective Switch L-Band (32WSS-L) card performs channel add/drop processing within the ONS 15454 DWDM node. The 32WSS-L works in conjunction with the 32DMX-L to implement ROADM functionality within the L band (1570 to 1620 nm). The 32WSS-L card is

particularly well suited for use in networks that employ DS fiber or SMF-28 single-mode fiber. Equipped with ROADM functionality, the ONS 15454 DWDM can be configured to add or drop individual optical channels using CTC, Cisco MetroPlanner, and CTM.

A ROADM NE utilizes two 32WSS-L cards (two slots each) and two 32DMX-L cards (one slot each), for a total of six slots in the chassis. The 32WSS-L card can be installed in Slots 1 and 2, 3 and 4, 5 and 6, 12 and 13, 14 and 15, or 16 and 17.

The 32WSS-L has six types of ports:

- ADD RX ports (1 to 32)
- EXP RX port
- EXP TX port
- COM TX port
- DROP TX port

For more details on the functions of the ports, see the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Several photodiodes monitor the power for the 32WSS-L card. The returned power level values are calibrated to the ports. See the *Cisco ONS 15454 DWDM Installation and Operations Guide* for more details.

32DMX-L Demultiplexer Card

The 32-Channel Demultiplexer L-Band card (32DMX-L) is a single-slot optical demultiplexer. The card receives an aggregate optical signal on its COM RX port and demultiplexes it into to 32 100-GHz-spaced channels. The 32DMX-L card is particularly well suited for use in networks that employ DS fiber or SMF-28 single-mode fiber. The 32DMX-L card can be installed in Slots 1 to 6 and in Slots 12 to 17.

The 32WSS-L has two types of ports:

- COM RX port
- DROP ports (1 to 32)

For more details on the functions of the ports, see the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Several photodiodes monitor the power for the 32WSS-L card. The returned power level values are calibrated to the ports. See the *Cisco ONS 15454 DWDM Installation and Operations Guide* for more details.

CE-1000-4 Card

The CE-1000-4 card, new for Release 7.0.x, uses pluggable Gigabit Interface Converters (GBICs) to transport Ethernet traffic over a SONET network. The CE-1000-4 provides four IEEE 802.3-compliant, 1000-Mbps Gigabit Ethernet ports at the ingress. At the egress, the CE-1000-4 card provides an integrated Ethernet over SONET mapper with four virtual ports to transfer Ethernet packets over a SONET network.

The Ethernet ports automatically configure to operate at either half or full duplex and can determine whether to enable or disable flow control. The Ethernet ports can also be oversubscribed using flow control.

CE-1000-4 card Ethernet frames are encapsulated using the ITU-T generic framing procedure (GFP) (with or without CRC) or LEX, the point-to-point protocol (PPP) with high-level data link control (HDLC). The CE-1000-4 card can interoperate with G1000-4/G1K-4 cards (using LEX encapsulation), CE-100T-8 cards (using LEX or GFP-F), and ML-Series cards (using LEX or GFP-F).

The Ethernet frames can be mapped into:

- T1X1 G.707-based high-order virtual concatenated (HO VCAT) payloads
- STS-3c-nv where n is 1 to 7
- STS-1-nv where n is 1 to 21
- Contiguously concatenated (CCAT) SONET payloads
- Standard CCAT sizes (STS-1, STS-3c, STS-12c, STS-24c, STS-48c)
- Non-standard CCAT sizes (STS-6c, STS-9c, STS-18c)

The CE-1000-4 card provides multiple management options through Cisco Transport Controller (CTC), Cisco Transport Manager (CTM), Transaction Language 1 (TL1), and Simple Network Management Protocol (SNMP).

The CE-1000-4 card supports the software link capacity adjustment scheme (SW-LCAS). This makes it compatible with the ONS 15454 CE-100T-8 and ML-Series cards. The CE-1000-4 card supports VCAT groups (VCGs) that are reconfigurable when SW-LCAS is enabled (flexible VCGs). The CE-1000-4 card does not support the standard hardware-based LCAS. For specific guidelines that apply to flexible VCGs consult the user documentation.

The CE-1000-4 card supports a non link capacity adjustment scheme (no-LCAS). This also makes it compatible with the ONS 15454 CE-100T-8 and ML-Series cards. The CE-1000-4 card supports VCAT groups (VCGs) that are fixed and not reconfigurable when no-LCAS is enabled (fixed VCGs). For specific guidelines that apply to fixed VCGs consult the user documentation.

The CE-1000-4 card supports VCAT differential delay and provides these associated features:

- Supports a maximum VCG differential delay of 122 ms in each direction.
- Supports all protection schemes (UPSR, two-fiber BLSR, four-fiber BLSR) on VCAT circuits that are split-fiber routed.
- Supports 2-fiber on VCAT circuits that are common-fiber routed.
- Differential delay compensation is automatically enabled on VCAT circuits that are diverse (split fiber) routed and disabled on VCAT circuits that are common-fiber routed.

For CE-1000-4 Card-Level Indicators, Port-Level Indicators, and Cross-Connect and Slot Compatibility, consult the user documentation.

MS-ISC-100T Card

The Multishelf Internal Switch Card (MS-ISC-100T) is an Ethernet switch used to implement the MSTP multishelf LAN. It connects the node controller shelf to the network and to subtending shelves. The MS-ISC-100T must always be equipped on the node controller shelf; it cannot be provisioned on a subtending controller shelf.

Cisco recommends that you configure the node to implement LAN redundancy, using two MS-ISC-100T cards: one switch is connected to the Ethernet front panel port of the TCC2/TCC2P card in Slot 7, and the other switch is connected to the Ethernet front panel port of the TCC2/TCC2P card in Slot 11. The Ethernet configuration of the MS-ISC-100T card is part of the software package and is automatically

loaded. The MS-ISC-100T card operates in Slots 1 to 6 and 12 to 17 on the node controller shelf; the recommended slots are Slot 6 and Slot 12. For MS-ISC-100T card port assignments and card-level indicators consult the user documentation.

MMU Card

The Mesh/Multiring Upgrade Unit (MMU) card supports multiring and mesh upgrades for ROADM nodes in both the C band and the L band. Mesh/multiring upgrade is the capability to optically bypass a given wavelength from one section of the network or ring to another one without requiring 3R regeneration. In each node, install two MMUs, one on the east side and one on the west side. You can install the MMU card in Slots 1 through 6 and 12 through 17.

The MMU has six ports:

- EXP RX port—The EXP RX port receives the optical signal from the ROADM section available on the NE.
- EXP TX port—The EXP TX port sends the optical signal to the ROADM section available on the NE.
- EXP-A RX port—The EXP-A RX port receives the optical signal from the ROADM section available on other NEs or rings.
- EXP-A TX port—The EXP-A TX port sends the optical signal to the ROADM section available on other NEs or rings.
- COM TX port—The COM TX port sends the optical signal to the fiber stage section.
- COM RX port—The COM RX port receives the optical signal from the fiber stage section.

For power monitoring, MMU card-level indicators, and MMU port-level indicators, consult the user documentation.

New Software Features and Functionality

CTC Support for Full C-band and L-band Trunk Wavelength Tunability

Release 7.0.x CTC supports full C-band and L-band trunk wavelength tunability with settings in the card-level Provisioning > Line > Wavelength Trunk Settings tab for the following cards:

- TXP_MR_10E_C
- TXP_MR_10E_L
- MXP_MR_10DME_C
- MXP_MR_10DME_L
- MXP_2.5G_10E_C
- MXP_2.5G_10E_L

Each card can be provisioned to operate in a specific trunk wavelength in its respective band (C or L). You can also preprovision trunk wavelength settings to the band appropriate for the card you plan to install. Trunk wavelength settings employ interleaved odd and even 100-GHz ITU spaced grids. Interleaved odd and even wavelength subdivisions ensure maximum transmission capacity in the form of a high number of available channels per card for your DWDM network, while also maintaining signal reliability. In CTC, selecting the odd or even grid sets your first tunable wavelength, as well as the 100-GHz ITU spaced wavelengths you can tune to thereafter.

Multishelf Nodes

Release 7.0.x supports multishelf DWDM nodes. Multishelf node provisioning enables you to centralize many tasks, such as node configuration and maintenance, VLAN management, software download, alarm management, performance monitoring, remote DCC, GCC, and OSC terminations, and database and diagnostic functions.

An ONS 15454 node provisioned as a multishelf node can manage up to 8 subtending shelves as a single entity. The node controller is the main shelf; its TCC2/TCC2P cards run multishelf functions. Each subtending shelf must also be equipped with TCC2/TCC2P cards, which run the local shelf functions. For internal data exchange between the node controller shelf and subtending shelves, the node controller shelf must be equipped with redundant MS-ISC-100T cards or, as an alternative, the Cisco Catalyst 2950 switch. Cisco recommends using the MS-ISC-100T cards. If you use the Catalyst 2950, install it on one of the multishelf racks. All subtending shelves must be located in the same site at a maximum distance of 100 meters from the Ethernet switches used to support the communication LAN.

A multishelf node has a single public IP address for all client interfaces (CTC, TL1, SNMP, or HTTP, for example); a client can only connect to the node controller shelf; not to the subtending shelves. The user interface and subtending shelves are connected to a patch panel using straight-through (CAT 5) LAN cables.

The node controller shelf has the following responsibilities:

- IP packet routing
- Network topology discovery
- Centralized OSPF

Subtending shelves have the following responsibilities:

- Overhead circuit management

Note To use overhead bytes, the AIC-I must be installed on the subtending shelf where it is terminated.

- Act as a single shelf node that can be used as a timing source line, TCC clock, or BITs source line

Multishelf Node Setup

Cisco recommend the following multishelf configurations, which are supported by MetroPlanner and automatically discovered by the software:

- Typical installation—All optical units are equipped on the node controller shelf, and TXP/MXP cards are equipped in the aggregated subtended shelves. In addition, all empty slots in the node controller shelf can be equipped with TXP/MXP cards.
- East/west protected—All optical units facing west are equipped in one shelf; all optical units facing east are equipped in another shelf.

Patchcords are automatically created only if the TXP/MXP cards have been previously tuned on one of the supported wavelengths.

DCC, GCC, and OSC Terminations

A multishelf node provides the same communication channels as a single shelf MSTP node:

- OSC links terminate on OSCM/OSC-CSM cards. Two links between each ONS node are required. An OSC link between two nodes cannot be substituted by an equivalent GCC or DCC link terminated on the same pair of nodes. OSC links are mandatory and they can be used to connect a node to a GNE.
- GCC and DCC links terminate on TXP or MXP cards.

The maximum number of DCC, GCC, and OSC terminations that are supported in a multishelf node is 48.

ROADM Multishelf Configuration Alarming

In Release 7.0.x, reconfigurable optical add-drop multiplexing (ROADM) systems can share a single IP address among shelves and also correlate optical signal alarms.

DWDM Network-Level Alarm Correlation

Release 7.0.x, ITU-T G.798-based alarm correlation simplifies alarm reporting for MSTP channels. Communication failures including Loss of Signal (LOS), Loss of Signal Payload (LOS-P), and Optical Power Receive Fail-Loss of Light (OPWR-LFAIL) generate multiple conditions at each affected node for each affected channel. Correlation simplifies troubleshooting because a single alarm is reported for each root cause. (The original alarms retain their severity in the Conditions window.)

The Payload Missing Indication (PMI) condition is raised at the far end to correlate OMS and OTS communication failures. A single PMI condition is sent when every channel on the aggregated port is lost, that is, when there are no pass-through channels or active added channels in service. If there are added channels on the node, the Forward Defect Indication (FDI) condition is raised at the near end to indicate there are no pass-through optical channels (OCH) in service.

Multishelf Ethernet Alarm Management

Ethernet alarm-raising for multishelf configuration also differs from the alarm-raising in single-shelf configurations. The shelf-connecting Ethernet interface card (MS-ISC-100T) does not raise traditional Ethernet alarms, such as CARLOSS, that apply to TXP or MXP client ports. Instead, MS-ISC-100T alarms are raised on the shelf as EQPT alarms. These alarms, new for Release 7.0.x, include Duplicate Shelf ID (DUP-SHELF-ID) and Shelf Communication Failure (SHELF-COMM-FAIL).

Viewing ROADM Alarmed Entities

The Multishelf view, added in Release 7.0.x, shows where an alarm is raised in the Object column. In Shelf view, the Alarms and Conditions tabs also contain a Shelf column that indicates where the alarmed card is located.

Optical Channel Trail and Client Connection Circuits

With Release 7.0.x the ONS 15454 MSTP system provides three types of optical channel circuits.

An Optical Channel Trail (OCH trail) is an optical circuit from a TXP/MXP trunk port to a TXP/MXP trunk port that can pass through a DWDM cloud, functioning as the server layer. Wavelength and signal rate are the OCH trail primary characteristics.

An Optical Channel Client Connection (OCHCC) is an optical channel from a TXP/MXP client port to a TXP/MXP client port. OCHCCs use the OCH trail as the server layer. OCHCCs are essentially client-to-client-circuits. Signal rate is the primary characteristic.

An Optical Channel Network Connection (OCHNC) is an optical circuit from an optical channel card to an optical channel card. Wavelength is the primary characteristic. OCHNCs are the legacy optical channel circuit type used in situations when OCH trails are not supported. OCHNCs are also used to carry wavelengths from non-ONS 15454 equipment.

Optical Channel Client Connection Functionality

Optical Channel Client Connections (OCHCCs) support SONET/SDH, Ethernet, FC/FICON, data storage (including ESCON), video, and passthrough (other) payload types. For specific payload rates, consult the user documentation.

You can upgrade existing OCHNCs created in earlier software releases to OCHCCs using the Circuits > Upgrade OCHNC option.

You can create DWDM OCHCCs by assigning port names, creating and verifying PPCs, verifying OCHCC client ports, and provisioning optical channel client connections as needed; or delete existing OCHCCs by deleting the associated optical channel network connections.

You can verify the provisionable patchcords (PPCs) that are required between client and optical channel nodes for OCHCCs using the Provisioning > Provisionable Patchcords (PPC) tabs.

When creating OCHCC circuits, on the Attributes page, you can define the following client circuit attributes:

- Name—Assign a name to the OCHCC. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Type—(Display only) OCHCC.
- Size—Defines the circuit payload type and rate. Two fields are provided. The first specifies the payload type. Choose a payload type, then choose the rate in the next field. The payload type and rate must match the PPM provisioning on the client cards at the source and destination nodes.
- OCHNC Wavelength—Provides three fields to define the wavelength that the OCHCC will use to travel across the OCH network. Choose a wavelength from the first field. In the second field, you can change the wavelength band by choosing either C Band or L Band. In the third field, you can indicate whether odd or even C-band or L-band wavelengths are displayed.
- Bidirectional—(Display only) OCHCCs are bidirectional. This field cannot be changed.
- State—Provisions the OCHCC state. The state can be IS (ANSI)/Unlocked (ETSI) or OOS,DSBLED (ANSI)/Locked,Disabled (ETSI).
- Apply to OCHCC ports—If checked, applies the state chosen in the next field to the OCHCC client ports. For TXP, MXP, TXPP, or MXPP cards, this will be the client and all trunk ports. For ITU line cards, this will be the trunk port only. The states that you can apply include: IS (ANSI)/Unlocked (ETSI), OOS,DSBLED (ANSI)/Locked,Disabled (ETSI), and IS,AINS (ANSI)/Unlocked,AutomaticInService (ETSI).
- Protection—Check this box if the source and destination client cards are TXPP or MXPP cards. Checking the box restricts the source and destination choices to those cards and allows you to provision the reversion parameters.
- Reversion—If Protection is checked, checking this box turns on the TXPP or MXPP reversion parameter.
- Reversion Time—If Reversion is checked, set the time before the protection will switch to the active port after conditions that caused the switch are remedied.
- G.709 OTN—If checked, enables the ITU-T G.709 optical transport network on the client cards, if permitted by the client card and payload.

- FEC—Allows you to enable or disable FEC on the client cards, if permitted by the client card and payload.
- SF BER—Allows you to set the signal fail bit error rate for payloads and client cards that allow the parameter to be provisioned.
- SD BER—Allows you to set the signal degrade bit error rate for payloads and client cards that allow the parameter to be provisioned.
- Mapping—Sets the mapping for cards that allow this parameter to be provisioned, including the TXP_MR_10E and MXP_MR_10DME cards. If you set mapping to Synchronous, the client signal is mapped into the OTU2 signal without justification of the payload because the client signal timing (the timing source) is the same as the trunk output timing. If you set mapping to asynchronous, the trunk timing is disconnected from the client timing (because the network element [NE] is the timing source), so justification is needed to map the client signal (OC192) to OTU2 trunk output.

Automatic Node Provisioning

Release 7.0.x offers a better solution for provisioning DWDM nodes, using Cisco MetroPlanner configuration files and connection reports.

Cisco MetroPlanner Configuration File Support

With Release 7.0.x you can import a Cisco MetroPlanner configuration file, provided in XML format, that provisions the shelf layout, sets the OPT-AMP-L mode (if present) and installs the automatic node setup (ANS) parameters calculated by Cisco MetroPlanner.

In CTC node view (for single-shelf mode) or multishelf view, you can access the configuration file from the Provisioning > WDM-ANS > Node Setup tabs. Each node setup session also monitors your setup process by maintaining a log file that you can view to see the results of your setup.

In the node setup page, you can choose from the following options. Each option will result in a different wizard guiding you through the steps to successful node setup.

- Provision Node Layout—Preprovisions the slots in CTC for the cards required by the network plan. Choose this option when no DWDM cards are installed. Preprovisioning the slots before the physical cards are installed ensures that card installers place the cards in the correct slots. Preprovisioning the slots is also useful if you want to set up the network prior to card installation.
- Provision Card Parameters—This option is available only when an OPT-AMP-L card will be installed. If you check the box, ANS provisions the OPT-AMP-L role, either as an L-band booster amplifier (OPT-LINE) or an L-band preamplifier (OPT-PRE).
- Provision ANS Parameters—If checked, installs the ANS parameters. ANS parameters provision the values required for the node to function within the specified network design. ANS parameters include span losses, optical power, optics thresholds, amplifier working mode, gain, tilt, and many others. Refer to the “Node Reference” chapter in the Cisco ONS 15454 DWDM Reference Manual for a list of ONS 15454 ANS parameters.
- Skip Interactive Mode—If checked, ANS provisions all the chosen setup components automatically without allowing you to view the results after each one.

Cisco MetroPlanner Internal Connections Report Support

With Release 7.0.x you can use the MetroPlanner Release 7.0 Internal Connections Report to install cables on your DWDM cards. The table displayed in the report identifies the patchcords that you must cable by their endpoints. Position 1 identifies the fiber start point; Position 2 indicates the fiber endpoint. The patchcord endpoints are identified by site, slot, and port. Information provided by the Internal Connections report includes:

- Site—Identifies the node where you are provisioning the internal connections.
- IP Address—The node IP address. The IP address will be 0.0.0.0 if it is not known.
- Position-1—The cable origination, in the format: Rack.Shelf.Port. Refer to the Cisco MetroPlanner Site Dialog for rack and shelf names and locations.
- Unit-1—The ONS 15454 DWDM card (unit) that is installed in the Position-1 slot. This is where the cabling originates.
- Port#-1—The port identifier shown in CTC for the first Position-1 connection.
- Port ID-1—The port identifier shown in TL1 for the Position-1 connection.
- Port Label-1—The name of the physical port printed on the card's front panel and shown in CTC card view for the Position-1 connection.
- Attenuator—If attenuation is required, the product ID of the bulk fixed attenuator is shown.
- Position-2—The cable termination, in the format: Rack.Shelf.Port. Refer to the Cisco MetroPlanner Site Dialog window for rack and shelf names and locations.
- Unit-2—The ONS 15454 DWDM card that is installed in the Position-2 slot. This is where the cabling terminates.
- Port #2—The port identifier shown in CTC for the first Position-2 connection.
- Port ID-2—The port identifier shown in TL1 for the Position-2 connection.
- Port Label-2—The name of the physical port printed on the card's front panel and shown in CTC card view for the Position-2 connection.
- Manually Set—Indicates whether you must create the connection manually in CTC. A Yes appearing in this column means that you must create the connection manually.

For detailed instructions on using the Cisco MetroPlanner Configuration Files and Internal Connections report, consult the user documentation.

MetroPlanner Support

Release 7.0.x supports MetroPlanner Release 7.0. For new features of MetroPlanner consult the MetroPlanner Release 7.0 documentation.

Server Trails

Release 7.0.x adds support for server trails. A server trail is a non-DCC link across a third-party network that connects two CTC network domains. A server trail allows circuit provisioning when no DCC is available. You can create server trails between any two optical or DS-3 ports. The end ports on a server trail can be different types (for example, an OC-3 port can connect to an OC-12 port). Server trails are not allowed on DCC-enabled ports.

The server trail link is bidirectional and can be VT1.5, VT2, STS1, STS-3c, STS-6c, STS-12c, STS-48c, or STS-192c; you cannot upgrade an existing server trail to another size. A server trail link can be one of the following protection types: Preemptible, Unprotected, and Fully Protected. The server trail protection type determines the protection type for any circuits that traverse it. PCA circuits will use server trails with the Preemptible attribute.

When creating circuits or VCATs, you can choose a server trail link during manual circuit routing. CTC can also route circuits over server trail links during automatic routing. VCAT common-fiber automatic routing is not supported.

BLSR STS and VT Squelching

Release 7.0.x supports BLSR STS squelching for the ONS 15454, ONS 15327, and ONS 15600, and VT squelching for the ONS 15454, and ONS 15327, with limited VT squelching support (see below) provided by the ONS 15600. STS-level squelching is supported in previous releases. With VT-level squelching added in Release 7.0.x the STS squelch table now displays VT-access status for each STS (every entry) in the table. There is a check box in both the east and west sides for each entry of STS squelch table, and a check mark in this box indicates that the STS is VT-access.

Release 7.0.x nodes display STS and VT squelch tables depending on the type of circuits created. For example, if a fiber cut occurs, the BLSR squelch tables show STSs or VTs that will be squelched for every isolated node. Squelching replaces traffic by inserting the appropriate alarm indication signal path (AIS-P) and prevents traffic misconnections. For an STS with a VT-access check mark, the AIS-P will be removed after 100 ms.

BLSR STS Squelch Tables in CTC

BLSR STS squelch tables show STSs that will be squelched for every isolated node. BLSR STS numbers, East and West source and destination information, and East and West incoming, or outgoing VT access indications are displayed in the BLSR Squelch Table window. BLSR squelching is performed on STSs that carry STS circuits only. Squelch table entries will not appear for STSs carrying VT circuits or Ethernet circuits to, or from E-Series Ethernet cards provisioned in a multicard Ethergroup. These squelch tables contain entries with adjacent node IDs displayed, instead of source or destination node IDs.

BLSR VT Squelch Tables in CTC

BLSR VT squelch tables only appear on the node dropping VTs from a BLSR and are used to perform VT-level squelching when a node is isolated. VT squelching is supported on the ONS 15454 and the ONS 15327 platforms. The ONS 15600 platform does not support VT squelching; however, when an ONS 15454 and an ONS 15600 are in the same network, the ONS 15600 node allows the ONS 15454 node to carry VT circuits in a VT tunnel. The ONS 15600 performs 100-ms STS-level squelching for each VT-access STS at the switching node in case of a node failure.

When using a VT circuit on a VT tunnel (VTT), or on a VT aggregation point (VAP), the VTT or VAP allows multiple VT circuits to be passed through on a single STS without consuming VT matrix resources on the cross-connect card.

In case of a source and destination node failure of a VTT, the switching node performs 100-ms STS-level squelching for the VTT STS. The node dropping VT traffic performs VT-level squelching. VT traffic on the VTT that is not coming from the failed node is protected.

An STS grooming node (VAP source) does not carry VT circuits through a VTT. The STS grooming node performs STS-level squelching for each STS timeslot at the switching node in case the VT-grooming (VAP destination) node fails. The node dropping VT traffic performs VT-level squelching for each VT timeslot in case the STS-grooming end node fails. No VT traffic on the VAP is protected during a failure of the STS-grooming node or the VT-grooming node.

The VT squelch table provides BLSR VT group number and channel indications, and East and West source information. To view the VT squelch table, double-click the STS with a check mark in the BLSR STS squelch table window. The check mark appears on every VT-access STS; however, the VT-squelch table appears only by double-clicking the check mark on the node dropping the VT. The intermediate node of the VT does not maintain the VT-squelch table.

"Ring is Squelching STS Traffic" Condition

Release 7.0.x supports an informational Ring is Squelching STS Traffic (STS-SQUELCH-L) condition that can be raised on an OC-N facility. The STS-SQUELCH-L condition indicates that traffic is squelched due to node failure (traffic outage). If the node failure scenario includes the source or destination node, then switching the nodes that switched the traffic away from the failure will squelch all the STSs that originate from or are destined to the failure node. The condition resolves when the node is no longer failing.

"Ring is Squelching VT Traffic" Condition

Release 7.0.x supports an informational Ring is Squelching VT Traffic (VT-SQUELCH-L) condition that can be raised on an OC-N facility. The VT-SQUELCH-L condition indicates that traffic is squelched due to node failure (traffic outage). If the node failure scenario includes the source node, the node dropping VT will squelch VT traffic. The condition resolves when the node failure is recovered.

Link Consolidation

CTC provides the ability to consolidate the DCC, general communications channel (GCC), optical transport section (OTS), server trail, and provisionable patchcord (PPC) links shown in the network view into a more streamlined view. Link consolidation allows you to condense multiple internodal links into a singular link. The link consolidation sorts links by class, meaning that all DCC links are consolidated together, for example. You can access individual links within consolidated links using the right-click shortcut menu. Each link has an associated icon.

Link consolidation is only available on non-detailed maps. Non-detailed maps display nodes in icon form instead of detailed form, meaning the nodes appear as rectangles with ports on the sides. Refer to the *Cisco ONS 15454 Procedure Guide* for more information about consolidated links.

Data Communications Network Tool

Release 7.0.x CTC includes a data communications network (DCN) tool that assists with network troubleshooting for Open Shortest Path First (OSPF) networks. This tool, located in network view, executes an internal dump command to retrieve information about all nodes accessible from the entry point. The retrieved information is the same as you would get if you were to execute a dump using special networking commands. The contents of the dump file can be saved or printed and furnished to Cisco Technical Support for use in OSPF network support.

Advanced Circuit Filtering and Export

Release 7.0.x adds an Advanced tab to the Circuit Filter dialog. With advanced circuit filtering you can filter on selected rings, nodes, links, or source/drop combinations.

Also, you can export the active Circuit window data in HTML, comma-separated values (CSV), or tab-separated values (TSV) format using the Export command from the File menu.

Superuser Privileges for Provisioning Users

With Release 7.0.x Superusers can grant permission to Provisioning users to perform a set of tasks, including retrieving the audit log, restoring a database, clearing performance monitoring (PM) parameters, activating a software load, and reverting a software load. These privileges can only be set using the node-level network element (NE) defaults, with the exception of the PM clearing privilege, which can be granted to a Provisioning user from the CTC Provisioning > Security > Access tabs. For more information about setting up Superuser privileges, refer to the *Cisco ONS 15454 Procedure Guide*.

CTC Download Highest Level NET JAR File

As of Release 7.0.x CTC, during network topology discovery, polls each node in the network to determine which one contains the most recent version of the CTC software. If CTC discovers a node in the network that has a more recent version of the CTC software than the version you are currently running, CTC generates a message stating that a later version of CTC has been found in the network, and offers to install the CTC software upgrade JAR files. If you have network discovery disabled, CTC will not seek more recent versions of the software. Unreachable nodes are not included in the upgrade discovery.

Local Domain Creation and Viewing

With Release 7.0.x a Superuser can control whether domains that any future users create and view persist globally (for all CTC sessions), or only locally (within the current CTC session in which they are created), as well as who can create domains (all users, or just Superusers). This control is given to Superusers by means of the NE default, CTC.network.LocalDomainCreationAndViewing. The factory pre-set default value is FALSE, meaning domain information is applied to all CTC sessions and only Superusers can create a domain or add a node to a domain. Setting the default to TRUE enables the option for local domain creation by any user.

Enhanced Fault Management

Release 7.0.x adds increased flexibility for fault management. When an entity is put in the OOS,MT administrative state, the node suppresses all standing alarms on that entity. All alarms and events appear on the Conditions tab. You can change this behavior for the LPBKFACILITY and LPBKTERMINAL alarms. To display these alarms on the Alarms tab, you can set the NODE.general.ReportLoopbackConditionsOnOOS-MTPorts to TRUE in the NE Defaults editor.

Rx and Tx Indication for TCAs

For electrical card or port PMs for which a direction, either Receive (Rx) or Transmit (Tx), can be detected, Release 7.0.x CTC and TL1 display the Rx or Tx value with the associated threshold crossing alert (TCA) description. For specific cards, port types, and PMs supported consult the Performance Monitoring chapter of the *Cisco ONS 15454 Reference Manual*.

TL1

New Card Support

The following new cards are supported by TL1 in Release 7.0.x.

- CE1000-4 Ethernet card
- MXP_MR_10DME-C and MXP_MR_10DME-L Multirate Muxponder cards
- TXP_MR_10E_C and TXP_MR_10E_L Multirate Transponder cards
- MXP_2.5G_10E_C and MXP_2.5G_10E_L cards
- MXP_MR_2.5G and MXPP_MR_2.5G demultiplexer cards
- MS-ISC-100T Data card
- MMU card

TL1 Command Changes

New Commands

The following new TL1 commands are added for Release 7.0.x.

- DLT-OCHNC
- ED-OCHNC
- ENT-OCHNC
- RTRV-OCHNC
- DLT-OCHCC
- ED-OCHCC
- ENT-OCHCC
- RTRV-OCHCC
- DLT-LNK
- ED-LNK
- ENT-LNK

Removed Commands

The following commands are removed from Release 7.0.x:

- DLT-WLEN
- RTRV-WLEN
- ED-WLEN
- ENT-WLEN

Command Syntax Changes

The syntax of the following commands is changed in Release 7.0.x.

ED-EQPT syntax:

ED-EQPT[:<TID>]:<aid>:<CTAG>[:::PROTID=<protid>,][PRTYPE=<prtype>,][RVRTV=<rvrtv>,][RVTM=<rvtm>,][CARDMODE=<cardmode>,][PEERID=<protid>,][REGENNAME=<regenname>,][PWL=<pwl>,][CMDMDE=<cmdmde>][:<pst>[,<sst>]];

Is changed to:

ED-EQPT[:<TID>]:<aid>:<CTAG>[:::PROTID=<protid>,][PRTYPE=<prtype>,][RVRTV=<rvrtv>,][RVTM=<rvtm>,][CARDMODE=<cardmode>,][PEERID=<peerid>,][REGENNAME=<regenname>,][CMDMDE=<cmdmde>,][RETIME=<retime>,][SHELFROLE=<shelfrole>,][NEWSHELFID=<newshelfid>][:<pst>[,<sst>]];

ED-GFP syntax:

ED-GFP[:<TID>]:<src>:<CTAG>[:::FCS=<fcs>,][AUTOTHGFPBUF=<autothgfpbuf>][GFPBUF=<gfpbuf>,][FILTER=<filter>];

Is changed to:

ED-GFP[:<TID>]:<src>:<CTAG>[:::FCS=<fcs>,][AUTOTHGFPBUF=<autothgfpbuf>,][GFPBUF=<gfpbuf>,][FILTER=<filter>];

ENT-EQPT syntax:

ENT-EQPT[:<TID>]:<aid>:<CTAG>::<aidtype>[:PROTID=<protid>,][PRTYPE=<prtype>,][RVRTV=<rvrtv>,][RVTM=<rvtm>,][CARDMODE=<cardmode>,][PEERID=<protid>,][REGENNAME=<regenname>,][PWL=<pwl>,][CMDMDE=<cmdmde>,][RETIME=<retime>][:];

Is changed to:

ENT-EQPT[:<TID>]:<aid>:<CTAG>::<aidtype>[:PROTID=<protid>,][PRTYPE=<prtype>,][RVRTV=<rvrtv>,][RVTM=<rvtm>,][CARDMODE=<cardmode>,][PEERID=<protid>,][REGENNAME=<regenname>,][CMDMDE=<cmdmde>,][TRANSMODE=<transmode>,][RETIME=<retime>,][SHELFROLE=<shelfrole>][:];

ENT-TADRMAP syntax:

ENT-TADRMAP[:<TID>]::<CTAG>:::TIDNAME=<name>,[IPADDR=<ipAddr>,][PORT=<port>,][ENCODING=<encoding>,][NSAP=<nsapAddr>];

Is changed to:

ENT-TADRMAP:[<TID>]::<CTAG>:::TIDNAME=<tidname>,[IPADDR=<ipaddr>],[PORT=<port>],[ENCODING=<encoding>],[NSAP=<nsap>];

INIT-SYS syntax:

INIT-SYS[:<TID>]:<aid>:<CTAG>[::];

Is changed to:

INIT-SYS[:<TID>]:<aid>:<CTAG>;

Note The INIT-SYS syntax change does not apply for CE-100T-8 cards.

OPR-SYNCNSW syntax:

OPR-SYNCNSW[:<TID>]::<CTAG>;

Is changed to:

OPR-SYNCNSW[:<TID>][:<aid>]:<CTAG>;

RTRV-NE-SYNCN syntax:

RTRV-NE-SYNCN[:<TID>]::<CTAG>[::::];

Is changed to:

RTRV-NE-SYNCN[:<TID>][:<aid>]:<CTAG>[::::];

RTRV-SYNCN syntax:

RTRV-SYNCN[:<TID>]:<aid>:<CTAG>[::::];

Is changed to:

RTRV-SYNCN[:<TID>][:<aid>]:<CTAG>[::::];

RTRV-TADRMAP syntax:

RTRV-TADRMAP[:<TID>][:<AID>]:<CTAG>:::MODE=<modeType>

Is changed to:

RTRV-TADRMAP[:<TID>][:<AID>]:<CTAG>[:::MODE=<modeType>]

ED-NE-GEN syntax:

ED-NE-GEN[:<TID>]::<CTAG>[:::NAME=<name>,][IPADDR=<ipaddr>,][IPMASK=<ipmask>,][DEFRTR=<defrtr>,][IIOPPORT=<iiopport>,][NTP=<ntp>,][SUPPRESSIP=<mode>];

Is changed to:

ED-NE-GEN[:<TID>]::<CTAG>[:::NAME=<name>,][IPADDR=<ipaddr>,][IPMASK=<ipmask>,][DEFRTR=<defrtr>,][IIOPPORT=<iiopport>,][NTP=<ntp>,][PROXYSRV=<isProxyServer>,][FIREWALL=<isFireWall>,];

ED-DS1 syntax:

ED-DS1[:<TID>]:<aid>:<CTAG>[:::TACC=<tacc>,][TAPTYPE=<taptype>,][MODE=<mode>,][FMT=<fmt>];

Is changed to:

ED-DS1[:<TID>]:<aid>:<CTAG>[:::TACC=<tacc>,][TAPTYPE=<taptype>,][AISONLPBK=<aisonlpbk>,][MODE=<mode>,][FMT=<fmt>];

Command Response Changes

The following TL1 responses have changed in Release 7.0.x.

ED-LNKTERM response:

::[<tmmd>],[<ssmgen>],[<qres>],[<rvrtv>],[<rvtm>]

Is changed to:

[<aid>]::[<tmmd>],[<ssmgen>],[<qres>],[<rvrtv>],[<rvtm>]

RTRV-EQPT response:

<aid>:<aidtype>,<equip>,[<role>],[<status>]:[<protid>],[<prtype>],[<rvrtv>],[<rvtm>],[<cardname>],[<ioscfg>],[<cardmode>],[<peerid>],[<regenname>],[<pwl>],[<transmode>],[<retime>]:<pst>,[<sst>]

Is changed to:

<aid>:<aidtype>,<equip>,[<role>],[<status>]:[<protid>],[<prtype>],[<rvrtv>],[<rvtm>],[<cardname>],[<ioscfg>],[<cardmode>],[<peerid>],[<regenname>],[<transmode>],[<retime>],[<shelfrole>]:<pst>,[<sst>]

RTRV-INV response:

<aid>,<aidtype>::[<pn>],[<hwrev>],[<fwrev>],[<sn>],[<clei>],[<twl1=nwl in code>],[<pluginvendorid>],[<pluginpn>],[<pluginhwrev>],[<pluginfwrev>],[<pluginsn>],[<ilossref>],[<productId>],[<versionId>],[<fpgaVersion>]

Is changed to:

<aid>,<aidtype>::[<pn>],[<hwrev>],[<fwrev>],[<sn>],[<clei>],[<twl1=nwl in code>],[<pluginvendorid>],[<pluginpn>],[<pluginhwrev>],[<pluginfwrev>],[<pluginsn>],[<ilossref>],[<productId>],[<versionId>],[<fpgaVersion>],[<vendorId>]

RTRV-DS1 response:

<aid>::[<tacc>],[<taptype>],[<mode>],[<fmt>]

Is changed to:

<aid>::[<tacc>],[<taptype>],[<aisonlpbk>],[<mode>],[<fmt>]

TL1 ENUM Changes

TL1 ENUM Items Added or Removed

The following section, including Table 5 through Table 26, highlights ENUM items changed (added or removed) for Release 7.0.x, by ENUM type.

Table 5 EQUIPMENT_TYPE enum items added to Release 7.0.x

Enum Name	Enum Value
EQUIPMENT_TYPE_ET_UNKNOWN	“UNKNOWN”
EQUIPMENT_TYPE_ET_UNPROVISIONED	“UNPROVISIONED”
EQUIPMENT_TYPE_ET_32_DMX_L	“32-DMX-L”
EQUIPMENT_TYPE_ET_32_WSS_L	“32-WSS-L”
EQUIPMENT_TYPE_ET_CE_1000_4	“CE-1000-4”
EQUIPMENT_TYPE_ET_MMU	“MMU”
EQUIPMENT_TYPE_ET_MS_ISC_100T	“MS-ISC-100T”
EQUIPMENT_TYPE_ET_MXP_MR_10DME	“MXP-MR-10DME”
EQUIPMENT_TYPE_ET_OPT_AMP_L	“OPT-AMP-L”
EQUIPMENT_TYPE_ET_OPT_BST_L	“OPT-BST-L”
EQUIPMENT_TYPE_ET_RAN_SVC	“RAN-SVC”
EQUIPMENT_TYPE_ET_SHELF	“SHELF”

EQUIPMENT_TYPE is used in the following commands:

- CHG-EQPT
- ENT-EQPT

Table 6 MTU_TYPE enum items added to Release 7.0.x

Enum Name	Enum Value
MTU_1500	“1500”
MTU_10004	“10004”
MTU_1548	“1548”

MTU_TYPE is used in the following commands:

- ED-GIGE
- ED-POS

Table 7 CARDMODE enum items added to Release 7.0.x

Enum Name	Enum Value
CARDMODE_AMPL_BST	“AMPL-BST”
CARDMODE_AMPL_PRE	“AMPL-PRE”
CARDMODE_MXPMR10DME_4GFC	“MXPMR10DME-4GFC”
CARDMODE_MXPMR10DME_4GFC_FCGEISC	“MXPMR10DME-4GFC-FCGEISC”
CARDMODE_MXPMR10DME_FCGEISC	“MXPMR10DME-FCGEISC”
CARDMODE_MXPMR10DME_FCGEISC_4GFC	“MXPMR10DME-FCGEISC-4GFC”

CARDMODE is used in the following commands:

- ED-EQPT
- ENT-EQPT
- RTRV-EQPT

Table 8 CATEGORY enum items dropped from Release 7.0.x

Enum Name	Enum Value
CATEGORY_2R	“2R”
CATEGORY_BBE	“BBE”
CATEGORY_ESCON	“ESCON”
CATEGORY_FC	“FC”
CATEGORY_GE	“GE”
CATEGORY_ISC	“ISC”
CATEGORY_OCN	“OCN”
CATEGORY_UNPROV	“UNPROVISIONED”
CATEGORY_WBE	“WBE”

CATEGORY is no longer used in any command.

Table 9 FLOW enum items added in Release 7.0.x

Enum Name	Enum Value
FLOW_PASSTHRU	“PASSTHRU”

FLOW is used in the following commands:

- ED-GIGE
- RTRV-FSTE
- RTRV-G1000
- RTRV-GIGE

Table 10 MOD1PAYLOAD enum items added to Release 7.0.x

Enum Name	Enum Value
MOD1PAYLOAD_ISC1	“ISC1”
MOD1PAYLOAD_ISC3	“ISC3”
MOD1PAYLOAD_4GFC	“4GFC”
MOD1PAYLOAD_4GFICON	“4GFICON”
MOD1PAYLOAD_ISC3PEER1G	“ISC3PEER1G”
MOD1PAYLOAD_ISC3PEER2G	“ISC3PEER2G”
MOD1PAYLOAD_ISC3PEER2R	“ISC3PEER2R”
MOD1PAYLOAD_ISCCOMPAT	“ISCCOMPAT”

MOD1PAYLOAD is used in the following commands:

- RTRV-OCHCC

Table 11 MOD2 enum items dropped from Release 7.0.x

Enum Name	Enum Value
MOD2_M2_ISC1	“ISC1”
MOD2_M2_ISC3	“ISC3”
MOD2_M2_WLEN	“WLEN”

Table 12 MOD2 enum items added to Release 7.0.x

Enum Name	Enum Value
MOD2_M2_4GFC	“4GFC”
MOD2_M2_4GFICON	“4GFICON”
MOD2_M2_ISC3PEER1G	“ISC3PEER1G”
MOD2_M2_ISC3PEER2G	“ISC3PEER2G”
MOD2_M2_ISC3PEER2R	“ISC3PEER2R”

Table 12 MOD2 enum items added to Release 7.0.x (continued)

Enum Name	Enum Value
MOD2_M2_ISCCOMPAT	“ISCCOMPAT”
MOD2_M2_OCHCC	“OCHCC”
MOD2_M2_OCHNC	“OCHNC”

MOD2 is used in the following commands:

- RTRV-FFP-MOD2
- RTRV-LNK-MOD2LNK
- RTRV-NE-APC
- RTRV-NE-WDMANS
- RTRV-OCHTERM
- RTRV-TRC-OCH
- SCHED-PMREPT-MOD2

Table 13 MOD2ALM enum items dropped from Release 7.0.x

Enum Name	Enum Value
MOD2ALM_M2_ISC1	“ISC1”
MOD2ALM_M2_ISC3	“ISC3”
MOD2ALM_M2_WLEN	“WLEN”

Table 14 MOD2ALM enum items added to Release 7.0.x

Enum Name	Enum Value
MOD2ALM_M2_4GFC	“4GFC”
MOD2ALM_M2_4GFICON	“4GFICON”
MOD2ALM_M2_ISC3PEER1G	“ISC3PEER1G”
MOD2ALM_M2_ISC3PEER2G	“ISC3PEER2G”
MOD2ALM_M2_ISC3PEER2R	“ISC3PEER2R”
MOD2ALM_M2_ISCCOMPAT	“ISCCOMPAT”

MOD2ALM is used in the following commands:

- RTRV-ALM-MOD2ALM
- RTRV-COND-MOD2ALM

Table 15 MOD2B enum items dropped from Release 7.0.x

Enum Name	Enum Value
MOD2B_M2_ISC1	“ISC1”
MOD2B_M2_ISC3	“ISC3”

Table 16 MOD2B enum items added to Release 7.0.x

Enum Name	Enum Value
MOD2B_M2_4GFC	“4GFC”
MOD2B_M2_4GFICON	“4GFICON”
MOD2B_M2_ISC3PEER1G	“ISC3PEER1G”
MOD2B_M2_ISC3PEER2G	“ISC3PEER2G”
MOD2B_M2_ISC3PEER2R	“ISC3PEER2R”
MOD2B_M2_ISCCOMPAT	“ISCCOMPAT”

MOD2B is used in the following commands:

- ALS
- RTRV-ALM-ALL
- RTRV-ALM-BITS
- RTRV-ALM-EQPT
- RTRV-ALM-SYNCN
- RTRV-COND-ALL
- RTRV-COND-BITS
- RTRV-COND-EQPT
- RTRV-COND-SYNCN
- RTRV-PM-MOD2
- RTRV-TH-ALL
- RTRV-TH-MOD2

Table 17 MOD2O enum items dropped from Release 7.0.x

Enum Name	Enum Value
MOD2O_M2_ISC1	“ISC1”
MOD2O_M2_ISC3	“ISC3”

Table 18 MOD2O enum items added to Release 7.0.x

Enum Name	Enum Value
MOD2O_M2_4GFC	“4GFC”
MOD2O_M2_4GFICON	“4GFICON”
MOD2O_M2_ISC3PEER1G	“ISC3PEER1G”
MOD2O_M2_ISC3PEER2G	“ISC3PEER2G”
MOD2O_M2_ISC3PEER2R	“ISC3PEER2R”
MOD2O_M2_ISCCOMPAT	“ISCCOMPAT”

MOD2O is used in the following commands:

- RTRV-ALMTH-MOD2O

Table 19 MOD2_DATA enum items dropped from Release 7.0.x

Enum Name	Enum Value
MOD2_DATA_M2_ISC1	“ISC1”

Table 20 MOD2_DATA enum items added to Release 7.0.x

Enum Name	Enum Value
MOD2_DATA_M2_4GFC	“4GFC”
MOD2_DATA_M2_4GFICON	“4GFICON”
MOD2_DATA_M2_ESCON	“ESCON”
MOD2_DATA_M2_ISCCOMPAT	“ISCCOMPAT”

MOD2_DATA is used in the following commands:

- DLT-RMONTH-MOD2-DATA

Table 21 NE_MODE enum items added to Release 7.0.x

Enum Name	Enum Value
NE_MODE_MULTISHELF	“MULTISHELF”
NE_MODE_MULTISHELFETH	“MULTISHELFETH”
NE_MODE_SINGLESHELF	“SINGLESHELF”

NE_MODE is used in the following commands:

- ED-NE-GEN

Table 22 OPTICAL_WLEN enum items added to Release 7.0.x

Enum Name	Enum Value
OPTICAL_WLEN_WL_1529_55	“1529.55”
OPTICAL_WLEN_WL_1529_94	“1529.94”
OPTICAL_WLEN_WL_1530_73	“1530.73”
OPTICAL_WLEN_WL_1531_51	“1531.51”
OPTICAL_WLEN_WL_1532_29	“1532.29”
OPTICAL_WLEN_WL_1533_07	“1533.07”
OPTICAL_WLEN_WL_1533_47	“1533.47”
OPTICAL_WLEN_WL_1533_86	“1533.86”
OPTICAL_WLEN_WL_1534_64	“1534.64”
OPTICAL_WLEN_WL_1535_43	“1535.43”

Table 22 OPTICAL_WLEN enum items added to Release 7.0.x (continued)

Enum Name	Enum Value
OPTICAL_WLEN_WL_1536_22	“1536.22”
OPTICAL_WLEN_WL_1537_00	“1537.00”
OPTICAL_WLEN_WL_1537_40	“1537.40”
OPTICAL_WLEN_WL_1537_79	“1537.79”
OPTICAL_WLEN_WL_1538_58	“1538.58”
OPTICAL_WLEN_WL_1539_37	“1539.37”
OPTICAL_WLEN_WL_1540_16	“1540.16”
OPTICAL_WLEN_WL_1540_95	“1540.95”
OPTICAL_WLEN_WL_1541_35	“1541.35”
OPTICAL_WLEN_WL_1541_75	“1541.75”
OPTICAL_WLEN_WL_1542_54	“1542.54”
OPTICAL_WLEN_WL_1543_33	“1543.33”
OPTICAL_WLEN_WL_1544_13	“1544.13”
OPTICAL_WLEN_WL_1544_92	“1544.92”
OPTICAL_WLEN_WL_1545_32	“1545.32”
OPTICAL_WLEN_WL_1545_72	“1545.72”
OPTICAL_WLEN_WL_1546_52	“1546.52”
OPTICAL_WLEN_WL_1547_32	“1547.32”
OPTICAL_WLEN_WL_1548_12	“1548.12”
OPTICAL_WLEN_WL_1548_92	“1548.92”
OPTICAL_WLEN_WL_1549_32	“1549.32”
OPTICAL_WLEN_WL_1549_71	“1549.71”
OPTICAL_WLEN_WL_1550_52	“1550.52”
OPTICAL_WLEN_WL_1551_32	“1551.32”
OPTICAL_WLEN_WL_1552_12	“1552.12”
OPTICAL_WLEN_WL_1552_93	“1552.93”
OPTICAL_WLEN_WL_1553_33	“1553.33”
OPTICAL_WLEN_WL_1553_73	“1553.73”
OPTICAL_WLEN_WL_1554_54	“1554.54”
OPTICAL_WLEN_WL_1555_34	“1555.34”
OPTICAL_WLEN_WL_1556_15	“1556.15”
OPTICAL_WLEN_WL_1556_96	“1556.96”
OPTICAL_WLEN_WL_1557_36	“1557.36”
OPTICAL_WLEN_WL_1557_77	“1557.77”
OPTICAL_WLEN_WL_1558_58	“1558.58”
OPTICAL_WLEN_WL_1559_39	“1559.39”

Table 22 OPTICAL_WLEN enum items added to Release 7.0.x (continued)

Enum Name	Enum Value
OPTICAL_WLEN_WL_1560_20	“1560.20”
OPTICAL_WLEN_WL_1561_01	“1561.01”
OPTICAL_WLEN_WL_1561_42	“1561.42”
OPTICAL_WLEN_WL_1561_83	“1561.83”
OPTICAL_WLEN_WL_1570_83	“1570.83”
OPTICAL_WLEN_WL_1571_24	“1571.24”
OPTICAL_WLEN_WL_1571_65	“1571.65”
OPTICAL_WLEN_WL_1572_06	“1572.06”
OPTICAL_WLEN_WL_1572_48	“1572.48”
OPTICAL_WLEN_WL_1572_89	“1572.89”
OPTICAL_WLEN_WL_1573_30	“1573.30”
OPTICAL_WLEN_WL_1573_71	“1573.71”
OPTICAL_WLEN_WL_1574_13	“1574.13”
OPTICAL_WLEN_WL_1574_54	“1574.54”
OPTICAL_WLEN_WL_1574_95	“1574.95”
OPTICAL_WLEN_WL_1575_37	“1575.37”
OPTICAL_WLEN_WL_1575_78	“1575.78”
OPTICAL_WLEN_WL_1576_20	“1576.20”
OPTICAL_WLEN_WL_1576_61	“1576.61”
OPTICAL_WLEN_WL_1577_03	“1577.03”
OPTICAL_WLEN_WL_1594_22	“1594.22”
OPTICAL_WLEN_WL_1594_64	“1594.64”
OPTICAL_WLEN_WL_1595_06	“1595.06”
OPTICAL_WLEN_WL_1595_49	“1595.49”
OPTICAL_WLEN_WL_1595_91	“1595.91”
OPTICAL_WLEN_WL_1596_34	“1596.34”
OPTICAL_WLEN_WL_1596_76	“1596.76”
OPTICAL_WLEN_WL_1597_19	“1597.19”
OPTICAL_WLEN_WL_1597_62	“1597.62”
OPTICAL_WLEN_WL_1598_04	“1598.04”
OPTICAL_WLEN_WL_1598_47	“1598.47”
OPTICAL_WLEN_WL_1598_89	“1598.89”
OPTICAL_WLEN_WL_1599_32	“1599.32”
OPTICAL_WLEN_WL_1599_75	“1599.75”
OPTICAL_WLEN_WL_1600_17	“1600.17”
OPTICAL_WLEN_WL_1600_60	“1600.60”

Table 22 OPTICAL_WLEN enum items added to Release 7.0.x (continued)

Enum Name	Enum Value
OPTICAL_WLEN_WL_1601_03	“1601.03”
OPTICAL_WLEN_WL_1601_46	“1601.46”
OPTICAL_WLEN_WL_1601_88	“1601.88”
OPTICAL_WLEN_WL_1602_31	“1602.31”
OPTICAL_WLEN_WL_1602_74	“1602.74”
OPTICAL_WLEN_WL_1603_17	“1603.17”
OPTICAL_WLEN_WL_1603_60	“1603.60”
OPTICAL_WLEN_WL_1604_03	“1604.03”
OPTICAL_WLEN_WL_850	“850”

OPTICAL_WLEN is used in the following commands:

- ED-10GIGE
- ED-DWDM-CLNT
- ED-EQPT
- ED-FC
- ED-GIGE
- ED-OCH
- ED-OCN-TYPE
- ENT-EQPT
- RTRV-10GIGE
- RTRV-DWDM-CLNT
- RTRV-EQPT
- RTRV-FC
- RTRV-GIGE
- RTRV-LNK-MOD2LNK
- RTRV-OCH
- RTRV-OCN-TYPE

Table 23 PAYLOAD enum items dropped from Release 7.0.x

Enum Name	Enum Value
PAYLOAD_PT_ISC1	“ISC1”
PAYLOAD_PT_ISC3	“ISC3”

Table 24 PAYLOAD enum items added to Release 7.0.x

Enum Name	Enum Value
PAYLOAD_PT_4GFC	“4GFC”
PAYLOAD_PT_4GFICON	“4GFICON”
PAYLOAD_PT_ISC3PEER1G	“ISC3PEER1G”
PAYLOAD_PT_ISC3PEER2G	“ISC3PEER2G”
PAYLOAD_PT_ISC3PEER2R	“ISC3PEER2R”
PAYLOAD_PT_ISCCOMPAT	“ISCCOMPAT”

PAYLOAD is used in the following commands:

- ED-FAC
- RTRV-E4
- RTRV-STM1E

Table 25 SHELF_ROLE enum items added to Release 7.0.x

Enum Name	Enum Value
SHELF_ROLE_NC	“NC”
SHELF_ROLE_SC	“SC”

SHELF_ROLE is used in the following commands:

- ED-EQPT
- ENT-EQPT
- RTRV-EQPT

Table 26 WLEN_MODE enum items dropped from Release 7.0.x

Enum Name	Enum Value
WLEN_MODE_ADD	“ADD”
WLEN_MODE_DROP	“DROP”
WLEN_MODE_EXP	“EXP”

WLEN_MODE is no longer used in any command.

Related Documentation

Release-Specific Documents

- *Release Notes for the Cisco ONS 15454, Release 7.0*
- *Release Notes for the Cisco ONS 15454 SDH, Release 7.0.2*

- *Release Notes for the Cisco ONS 15327, Release 7.0.2*
- *Release Notes for the Cisco ONS 15600, Release 7.0.2*
- *Release Notes for the Cisco ONS 15310-CL, Release 7.0.2*
- *Release Notes for the Cisco ONS 15310-MA, Release 7.0.2*
- *Cisco ONS 15454 Software Upgrade Guide, Release 7.0*

Platform-Specific Documents

- *Cisco ONS 15454 Procedure Guide*
  Provides installation, turn up, test, and maintenance procedures
- *Cisco ONS 15454 Reference Manual*
  Provides technical reference information for SONET/SDH cards, nodes, and networks
- *Cisco ONS 15454 DWDM Installation and Operations Guide*
  Provides technical reference information for DWDM cards, nodes, and networks
- *Cisco ONS 15454 Troubleshooting Guide*
  Provides a list of SONET alarms and troubleshooting procedures, general troubleshooting information, and hardware replacement procedures
- *Cisco ONS SONET TL1 Command Guide*
  Provides a comprehensive list of TL1 commands

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/

Cisco Marketplace:

http://www.cisco.com/go/marketplace/

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

  http://www.cisco.com/en/US/partner/ordering/

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com
- Nonemergencies—psirt@cisco.com

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0609R)

Copyright © 2006, Cisco Systems, Inc.
All rights reserved.